Journal of Autonomous Intelligence (2024) Volume 7 Issue 2
doi: 10.32629/jai.v7i2.672

ORIGINAL RESEARCH ARTICLE

Artificial intelligence governance in smart cities: A European regulatory perspective

Brian Fabregue

Blue Europe, the Think Tank, Rue de Kokelscheuer, Esch-sur-Alzette 3323, Luxembourg; brianfranco.fabregue@uzh.ch

ABSTRACT

The integration of AI in our daily lives is rapidly increasing, offering numerous benefits to society. In a Smart City context, said integration is almost implicit: Smart Cities allow for a stream of data upon which AI is not only used but developed and trained. There are however concerns about the unpredictability and uncontrollability of AI, prompting calls for transparency and explainability of its underlying machine-learning algorithms. To ensure useful and understandable explanations of inherent biases, policymakers should focus on the concrete risks and biases of algorithms in relation to specific legal contexts. This article examines the legal implications of AI, including potential regulatory frameworks, the impact on privacy and intellectual property laws, and ethical issues. It also explores governance drivers and policy processes of AI regulation and governance in the European Union. Then, after focusing on the newest Artificial Intelligence Act—viewed both under a fundamental right and a smart city AI integration perspective, it is argued that a three principle-based approach to AI deployment in smart cities is needed to balance inefficiencies derived from the inherent complexity of AI, namely: fairness, privacy and transparency.

Keywords: artificial intelligence; smart cities; regulation; artificial intelligence act; Europe

ARTICLE INFO

Received: 30 May 2023
Accepted: 24 October 2023
Available online: 21 December 2023

1. Introduction

Taken as a whole, Artificial Intelligence (AI) poses threats to both individuals and potentially entire societies[1,2], especially in a Smart City[3,4]. Fundamental rights, such as the right to self-determination[5], privacy and protection of data[6], freedom of expression and assembly, non-discrimination, the right to an effective remedy and a fair trial, and consumer protection, may be violated by AI[7,8]. In particular, the articulation of AI problematics within the smart city revolves around itself in a self-feeding loop, as the more technology is deployed to solve and deal with urban complexities, the more complex a smart city ends up being, with even more issues to be addressed both legally and practically. These problematics are almost entirely related to the treatment of end users' data[9].

The legal implications of AI need to be considered by governments, businesses and individuals as the technology develops and becomes more sophisticated. With the proliferation of public transport, local taxes, police records, traffic sensors and weather stations, cities generate huge amounts of data. This type of information needs to be collected and analysed to produce results that can be used to improve a city. However, there is far more data in its raw form than anyone could ever hope to view, interpret or evaluate.

Artificial intelligence can process vast amounts of data from a variety of sources, enabling the discovery of insights that can be used to increase the effectiveness and efficiency of city operations while reducing associated costs. A significant portion of a city's public infrastructure is under-utilised, over-utilised or inefficiently utilised at any given time due to a lack of real-time data and tool to use it[10]. AI-powered smart city systems can collect and analyse data from a wide range of municipal services. In smart cities, a combination of AI and analytics based on data collected by sensors throughout the urban environment can solve a variety of problems, including traffic congestion and crime[11,12].

The globalisation of technology and its applications has given rise to numerous legal issues related to artificial intelligence. Robotics, machine learning and natural language processing are just a few examples of the many different types of technology that fall under the umbrella of AI. As AI technology advances, more challenging legal issues arise.

Since 2016, policymakers, industry, civil society, think tanks, media and consultancies around the world have been engaged in intense discussions about the types of policies and governance that would enable the development and socially beneficial use of artificial intelligence and help mitigate the associated risks[13–15]. Globally, according to the OECD Artificial Intelligence Index Report of 2021, more than 50 countries (including the European Union) have developed or are in the process of developing a national AI policy[16], while a 2019 global survey identified a total of 84 AI ethics guidelines[17].

These policy documents and ethics guidelines have been published in response to recent developments in artificial intelligence (AI), which is defined as a system that exhibits intelligent behaviour by analysing its environment and taking action[18]. While ground-breaking developments in the field of artificial intelligence (AI) occurred as early as the 1950s and 1960s, more recent advances in hardware and big data[19] have enabled the application of AI in a variety of fields, including education and health, as well as transportation[20] and the military[21].

Against a potential backdrop, the European Union (EU) has been actively debating how it can promote the creation and application of AI, what kind of AI it wants to create, and how it can contribute to the advancement of AI globally. Initially, the EU's main concern was that it would fall behind North America and Asia. According to the report "10 Imperatives for Europe in the Age of AI and Automation", written by McKinsey & Company for the EU Heads of State Tallinn Digital Summit in September 2017, Europe is making progress but still lags behind the US and China[22]. The report specifically notes that Europe as a whole is lagging behind in external AI investment, with total investment of $3 billion to $4 billion in 2016, compared with $8 billion to $12 billion in Asia and $15 billion to $23 billion in North America[22]. The report is significant and is cited in key EU documents on AI, including the 2020 AI white paper[23], the 2018 AI strategy[18] and the coordinated plan[24].

2. Defining artificial intelligence in a smart city context

Defining the subject matter of regulation is crucial from a legal regulatory perspective, as it defines the scope of the regulation itself. However, because so many different scientific disciplines are directly or indirectly affected by AI, as are so many different social groups, each perspective has its own interpretation of what AI is and what it means for that particular discipline. There is no widely accepted technical description of what artificial intelligence is or could be, as evidenced by the fact that neither computer science nor informatics are specifically addressed in the European Artificial Intelligence Act (AIA)[25].

Legal definitions must meet, to varying degrees, the following criteria: inclusiveness, precision, comprehensiveness, practicality and durability. Definitions are overbroad if they are too narrow in scope to achieve the regulatory objective, and under-broad if they cover matters that are not covered by the regulatory objective[26]. The principle of the rule of law calls for precision, thoroughness and practicability because of the need for the principles of proportionality, legal clarity, predictability and applicability of the law[27]. Permanence may seem at odds with the idea of future-proof legislation, but it is based on the legal principle that abstract general rules are created for a wide range of applications, rather than having to be applied to each individual case.

The difficulties defining AI in smart cities from a legal perspective begin with the lack of a "generalisable" or consistent definition of what artificial intelligence is across domains. Definitions of artificial intelligence (AI) have changed significantly over time, resulting in an extremely ambiguous term[26].

The difficulty in identifying AI is an example of how difficult it is to regulate technology and smart cities overall. Hence, the regulatory objective should be focused on the practical protection of legal rights as well as the dogmatic principles of fundamental rights. However, there are other ways to support the relevance of legally protected interests. The precautionary principle states that certain high-risk objects and processes should not be subject to additional requirements to bring them under legal control unless they pose a significant risk to important legal interests[28]. The problem with AI is that its impact is either insufficiently measurable, not yet measurable or not measurable at all[29]. This seems to be one of the reasons why many plans seem to focus more on the technology itself than on how it will affect people and legally protected interests. The proportionality principle states that the less factual information is provided, the more complex a predictive risk assessment must be.

Therefore, only the interplay between the technological functionality and the application context can be used to determine the risk profile of AI systems. The principle of proportionality and equal treatment requires that different systems be treated differently in terms of existing legal rights, as different systems have quite different risk profiles[30].

Defining the topic artificial intelligence dates back to 1956 when McCarthy first used the word "AI", later describing it as "the science and engineering of making intelligent machines"[31]. The concepts of acting humanely, thinking humanely, thinking rationally and acting rationally have been central to many subsequent definitions[32], for instance, AI is described in the Encyclopaedia Britannica as "the ability of a computer or a robot controlled by a computer to do tasks that are usually done by humans because they require human intelligence"[33]. These classic definitions all refer to intelligence in humans, which is just one example of how psychology, cognitive science and neuroscience have long been closely associated with artificial intelligence (AI)[34]. More recently, interdisciplinary studies have move forward the definition of AI, conjugating it with the smart city context. 'Urban AI' is in fact defined as the "relationship between artificial intelligence systems and urban contexts, including the built environment, infrastructure, places, people, and their practices"[35]. According to this advanced definition, there is a pressing need for a coordinated effort to investigate urban AI as an interdisciplinary research theme, which entails examining the connections between AI, the physicality of spaces, people's lives, and the ethical and political aspects of urban AI globally[36]. Urban AI may, in theory, have an impact on regional dynamics, city and state governance, and worldwide competitiveness between cities and states. It may also have an impact on the dynamism between urban, rural, and suburban areas. In order to completely understand these events, it is crucial to present relevant ideas, approaches, and associated research subjects from other domains.

The term "artificial Intelligence" (AI), however, is criticised from a humanities perspective, because intelligence is a natural human quality. It is said that because AI is not equivalent to human intellect, the term is politicised, imprecise or even untrue[37]. The question of what intelligence "actually" is and what philosophically feasible modes of decision making are at the forefront of the partly philosophical consideration of what AI might be. Since human intelligence is the measure most often used to evaluate machine intelligence, the concepts of human intelligence and machine development have long been intertwined. An AI is said to be intelligent if it is able to act in a way that humans would act, or even better[38].

Combining ideas from computer science and electrical engineering, artificial intelligence and decision-making develop methods for analysing and synthesising systems that engage with the outside world through perception, communication, and action in addition to learning, making decisions, and adapting to a changing environment. Duan et al. provide an extensive review of how decision making evolved within AI technologies thanks to the development of big data[39].

The words "decision automation", "decision augmentation", and "decision support" indicate the varying degrees to which AI and analytics may be utilised to seek faster, more reliable, more flexible, and higher-quality decisions at scale, especially in a workplace environment[40].

Artificial neural networks are used to simulate human computational and learning abilities; the main difference between the operation of neurons and human thinking is that neurons operate at a sub-symbolic level. On the other hand, conscious human thought seems to operate at a symbolic level[34].

Even ignoring the technological scope, different forms of intelligence[41] could lead to different definitions of AI. Thus, from a legal perspective, intelligence seems to be linked to a kind of autonomy (another hotly debated idea) resulting from the ability to adapt[42]. Against this background, the law currently takes into account several types of autonomy in the field of artificial intelligence (also known as "in the loop"), such as in Art. 22 of the General Data Protection Regulation (GDPR)[1]. These levels focus on the degree of human involvement in the AI-driven decision-making process. Because neither autonomy nor intelligence can be adequately defined, context-based definitions are the only way to create legal provisions that are consistent with legal certainty and the rule of law.

After all, AI systems raise very different issues depending on who, where and for what. Even if both use AI systems, it is difficult to compare, for example, an autonomous weapons system with a spam filter. In fact, this one example shows how pointless it would be for politicians to pass a comprehensive Artificial Intelligence Act that would regulate the whole phenomenon from the top down, under the control of an Artificial Intelligence Agency. It therefore seems that 'algorithms' and 'AI' do not need a single, all-encompassing definition, but policy makers should focus is more on different characteristics of different algorithms and AI applications, and how they are applied in practice[43].

Taken together, the current definitions of AI fall short of the most important needs for legal definition. They are highly ambiguous and overly inclusive, and it is questionable whether they are understandable or workable[26]. Any kind of regulation of AI is therefore hampered by the lack of a generally accepted definition[44]. Moreover, since the law is concerned with defining the danger of an AI, the applicability of a more restrictive meaning of the term is questionable. The fact that an AI meets the definition does not necessarily mean that its use is without risk[45].

3. The European approach to artificial intelligence regulation

Although AI has only recently become a focus of EU policy, concerns that the EU is falling behind the US and Asia (most recently China) in science, technology and innovation have been a key driver of European integration in research and technology policy since its inception in the 1950s, and were prominent in the launch of the European Research Area in 2000 and the Europe 2020 strategy for smart, sustainable and inclusive growth[46].

However, the following remark demonstrates how the EU seeks to set itself apart from the US and China by emphasizing its moral, human-centric, and value-based approach[47]:

> *"There is strong global competition on AI among the USA, China and Europe. The USA leads for now but China is catching up fast and aims to lead by 2030. For the EU, it is not so much a question of winning*

or losing a race but of finding the way of embracing the opportunities offered by AI in a way that is human-centred, ethical, secure, and true to our core values."

Many EU institutions and individuals have been involved in the development of EU policy on AI. The main EU policy documents on AI are listed chronologically in **Table 1**. In addition to these important achievements, numerous other papers and opinions from EU institutions[48], experts[49] and stakeholders[50] have contributed to in-depth discussions on the EU approach to AI[14,15].

Policy makers, stakeholders and experts have drawn inspiration from past examples of successful European integration, as well as developments in other countries and sectors, in developing an EU strategy. An overview of global projects from the US, China, Japan, the UK, Germany and the United Arab Emirates is included in the report of one of the European Commission's early AI policy seminars[51]. The seminar also proposed the creation of a CERN-style organisation for AI research, a large-scale facility that is seen as one of the major successes of European integration in research[52].

Table 1. Timeline of the European artificial intelligence regulation process.

Date	Institution	Description
Feb 2017	European Parliament	Recommendations on Civil Law Rules on Robotics[53]
Apr 2018	European Commission	Artificial Intelligence for Europe[18]
Dec 2018	European Commission	Coordinated Plan on Artificial Intelligence[24]
Apr 2019	European Commission	Ethics Guidelines for Trustworthy AI[54]
Feb 2020	European Commission	A European Approach to Excellence and Trust[23]
Apr 2021	European Commission	Fostering a European Approach to Artificial Intelligence[55]
Apr 2021	European Commission	Artificial Intelligence Act proposal[56]
Jun 2021	European Data Protection Board	Joint opinion with the Data Protection Supervisor[57]
Dec 2021	European Central Bank	Opinion on harmonised rules on AI[58]
Sep 2022	European Commission	AI Liability proposal[59]
Dec 2022	European Council	Final position on the AIA proposal[60]
May 2023	European Parliament	Position adopted by key committees on the AIA proposal[61]

3.1. The artificial intelligence act

Since at least 16 July 2019, artificial intelligence laws have been expected in Europe. On that day, Ursula von der Leyen made a commitment to propose new AI laws 100 days after her election as President of the European Commission.

According to the website of the European Data Protection Supervisor, the AIA is "the first initiative, worldwide, that provides a legal framework for Artificial Intelligence (AI)"[62]. Whether or not this is the case (for instance, the US National AI Initiative Act—2021), the AIA is one of the most significant regulatory actions taken to date on a global scale. A vision of AI that seeks to benefit the economy, society and the environment is generally a good starting point for ensuring that the development of AI in the EU is morally sound, legally acceptable, socially equitable and environmentally sustainable.

The EU is positioning itself as a single point of contact for AI applications, as well as for the management of personal data (GDPR). When demonstrating compliance with the new legislation, AI companies and providers will be dealing with the EU rather than individual Member States. Each Member State will designate a national authority responsible for the supervision of AI. To ensure consistent application of the AI Regulation, including the list of prohibited AI practices and high-risk systems, a new European Artificial Intelligence Board (EAIB) will work with national regulators and EU lawmakers. See **Figure 1** below for a hierarchical schematisation of the different risk levels presented in the AIA. The AIA will be incorporated into the GDPR, the Digital Services Act[63] and the Digital Markets Act[64], which, once passed, will regulate online platforms and services. In the end, we have to take all this into account. When this "legislative square" is completed, the EU will have created a "digital constitutionalism"[65] for an infosphere where its citizens can live and work better. Make it a pentagon if you add the Data Governance Act[66], or a hexagram with the legislative proposal on the European Health Data Space[67].

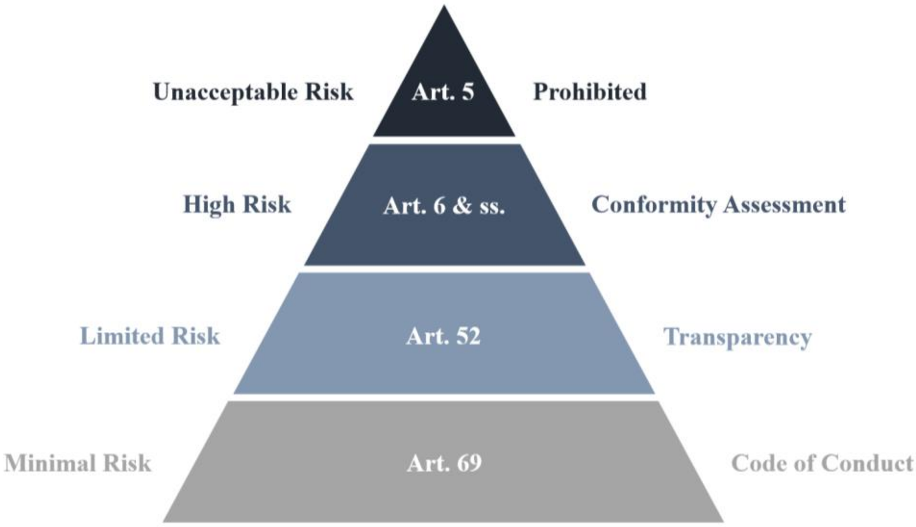

Figure 1. Artificial Intelligence Act Risk Levels (Source: Author compilation).

Without much surprise, the AIA regulation is structured in a similar fashion than the GDPR, without the regulatory power of the pan-European board. In this situation, too, one might expect a 'harmonising' effect, similar to that of the GDPR. An explicit and trusted legal framework will facilitate cooperation between the EU and other nations. While China and the US won't take the same approach as the EU, they still need to work with the EU. China may use the AIA as a model to develop legislation specific to its view of AI[68]. Roberts et al.[69] show that US is more likely to take an antitrust approach, but the AIA could have an impact on state-level legislation, as it did with the California Consumer Privacy Act[70]. A future EU-US Trade and Technology Council could also provide a common platform[71].

But what can we take from the AIA from a regulatory perspective? The fundamental approach of the GDPR, which is based on the defence of human dignity and fundamental rights, is carried over into the AIA from an ethical point of view. Even if the AIA (proposal) is less flexible, top-down and focused on protecting citizens' rights than the GDPR. This is still a core element of its legal lookout.

3.1.1. The artificial intelligence act: A smart city regulation?

Article 5 lists the forbidden usages of the AI: in its first paragraph, point (a)[2], what is known as nudging in a Smart City context, is directly targeted. Nudging is in fact a major problem in smart cities[72] and Art. 5 considerably addresses said practice. However, other known usages of AI in a smart city context that have been deemed doubtful are not listed in point (a), such as the surveillance and identification of citizens[73]—for instance on the Chinese model[74,75]. Point (b) and (c) theoretically target the above-mentioned usages, but point (d) provides broad and blanket exceptions[3] making the previous ban moot. It is interesting to note that Article 5(1) (a) (nudging) and (b) (discrimination) of the EU AI Act only address a small number of deficiencies. See **Table 2** below for the full description of AI practices prohibited by Art. 5 of the AIA.

Table 2. Prohibited AI practices by Art.5 of the Artificial Intelligence Act.

Manipulation of Behaviour	**Manipulation and Exploitation of Vulnerable Groups**	**Social Scoring**	**Biometric real-time identification**
Placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's behaviour consciousness with the objective to or the effect of materially distorting a person's behaviour in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm.	Placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age disability, or a specific social or economic situation, with the objective or the effect of materially distorting the behaviour of a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person physical or psychological harm.	Placing on the market, putting into service or use of AI systems for the evaluation or classification of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following: ● detrimental or unfavourable treatment of certain natural persons or groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected; ● detrimental or unfavourable treatment of certain natural persons or groups thereof that is unjustified or disproportionate to their social behaviour or its gravity.	The use of 'real-time' remote biometric identification systems in publicly accessible spaces by law enforcement authorities or on their behalf for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives: ● the targeted search for specific potential victims of crime; ● the prevention of a specific and substantial threat to the critical infrastructure, life, health or physical safety of natural persons or the prevention of a terrorist attacks; ● the detection, localisation, identification of a natural person for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for offences e referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, or other specific offences punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least five years, as determined by the law of that Member State.

Source: General Approach of the Council of the European Union (December 2022)[60].

Article 10, under the "high risk" AI (authorised with limits), allows the usage of public data, including public transport and personal data, if the data is not used for discrimination for specific categories.

This is, to say the least, a very doubtful choice, as the problem in the usage of public data is that it is mostly not consensual data. The article tries to limit the usage of said data (article 10 (5))[4], but the original instruments lack outright ban on usage of public data, especially when not immediately linked to an individual natural person.

The only provision in the EU AI Act that explicitly refers to Article 9 of the GDPR is indeed Article 10(5), but only to limit Article 9(1)'s ability to allow monitoring, detection and correction of bias in high-risk AI systems[76].

Therefore, while the EU AI law seeks to complement the GDPR and provide sufficient protection for individuals' fundamental rights to privacy and data protection, this goal remains aspirational for now.

Does the EU AI law really provide protection against violations of fundamental rights? The stated goal of the act was to establish full compliance with current EU law and to strengthen the protection of fundamental rights provided by EU secondary legislation such as the GDPR[77]. The GDPR was created to enhance the right to privacy and data protection in the digital age, but it is insufficient to comprehensively address the significant reliance of AI on personal data[78]. The EU AI Act seeks to address these gaps and harmonise with the GDPR through its Article 10 on data governance[78].

It is still debatable whether the two pieces of legislation work together effectively enough. For example, the GDPR's guidelines on data collection and processing are not explicitly included in the EU AI Act (GDPR, Articles 5–14, 16–18, 21). Additionally, without any mention of the GDPR, some broad and not easily achievable characteristics that data sets should have are listed in Article 10(3) of the EU AI Act and a somewhat ambiguous reference to data governance and management strategies is made in Article 10(2) of the EU AI Act[76].

The promotion of innovation and economic progress and the protection of fundamental rights are in competition within the Act, which is what makes it unique. The only way to resolve this internal conflict is for AI providers (i.e., AI developers and deployers) and users to comply with a set of strict requirements for the high-risk AI systems defined in Annexes II and III.

In reality, the way in which EU AI law assigns responsibility to AI companies and users compromises its approach to the protection of fundamental rights. Traditional thinking holds that fundamental rights serve to protect the individual from the state[79]. This view is supported by the EU AI Act, which sets out rules for AI providers and users to follow, yet it does not subject them to fundamental rights obligations. What the Act does is replace fundamental rights with some form of Transparency and accountability in the decision, namely article 13[5] on one side and 12–14 on the other. Additionally, the Act does not take into account the average usage of the AI in the smart city, which is both invisible and hard to grasp: as usages are linked to urbanism, the average user suffers from the Zeno's grain paradox perspective[6]. Sure, one very specific usage of the AIA may be hard to grasp, but thousands of them will have massive effects, while still impossible to distinguish one another.

The EU AI Act could be seen as a mediated way of protecting fundamental rights as a result. However, fundamental rights serve as a benchmark for interpretation. Given the serious risks posed by these systems, the requirements for AI providers and users to demonstrate compliance with the standards for high-risk AI systems appear weak from this perspective[80].

The governance, enforcement and redress mechanisms of the EU AI Act also appear to be ineffective[76]. It is primarily the provider's responsibility to determine ex ante whether a high-risk AI system complies with the requirements of Title III, Chapter 2 of the EU AI Act. Normally, this is a self-conformity assessment without external control[57,77]. As this is primarily the responsibility of the AI provider, the quality of the risk management system to be put in place under Article 9 of the EU AI Act may also differ.

Because of this lack of regulation, the EU AI Act gives AI providers a lot of leeway to make decisions that could potentially violate fundamental rights. Additionally, there does not seem to be an impartial organisation in charge of properly assessing whether the EU AI law has violated someone's fundamental rights. As a result, no one can ultimately be held accountable if administrators, users or providers break the law. People will therefore have to use other legal systems to seek justice, which may reduce their level of legal protection[76]. The EU AIA is, as such, very lacking, especially in a smart city context.

3.2. The emerging role of generative AI and EU law

Rapidly altering how we communicate, create, and work is generative AI. Its effects will inevitably permeate all facets of society, from commercial growth to medical, education to research, and from programming to entertainment and the arts. AI with generative capabilities has enormous potential, but also carries tremendous danger. Currently, millions of people rely on them to create human-level text (e.g., ChatGPT, Luminous, Bing), pictures (e.g., Stable Diffusion, DALL-E 2), videos (e.g., Synthesia), or audio (e.g., MusicLM), and further options are in the works[81].

Soon, they may be included into employment tools that score and respond to job applicants, or hospital administration systems that generate letters to patients based on case files. Such multi-modal decision engines may help to a more effective and equitable allocation of resources by allowing professionals more time to focus on substantive problems, such as real patient treatment[82]. Nonetheless, errors will be expensive, and hazards ranging from discrimination and privacy to insulting content must be addressed appropriately[83]. Already, the unrestrained capabilities of generative AIs may be utilised to elevate manipulation, false news, and damaging speech to a completely new level[84,85]. Consequently, the argument over how to regulate generative AI systems is intensifying[86,87].

In the EU and worldwide, AI policy has mostly concentrated on conventional AI models, not the next generation whose birth we are currently seeing. To more accurately reflect the reality of the expanding AI value chain, the terminology and duties under the AI Act and other relevant regulations should be revised. Some of these observations also apply to traditional AI systems; however, generative models are unique in that they produce output designed for communication or speech, which raises important and novel questions regarding the regulation of AI-enabled communication.

Generative AI systems and the AI act

The AI Act seeks to keep up with the rapid dynamics in the artificial intelligence technology sector. There are, however, a few reasons—some mentioned in Section 3.1.1—that show how recently established regulations do not do justice to the uniqueness of big AI models, particularly large generative AI models. First of all, as stated before, the term under Art. 3(1b) of the AI Act is excessively broad. Notably, they often work on a broader spectrum of situations than conventional models[88]. Conceptually, their "generality" may refer to their capability; domain of use cases and breadth of tasks covered[89]. Generative AI systems, in our opinion, must inevitably exhibit a high degree of generality in terms of its capabilities, tasks, and outputs, beyond the mere fact that they may be incorporated into several use cases (which also holds true for extremely simple algorithms). Nonetheless, the expansive definition of Generative AI systems under the AI Act (Council general approach) conflicts with this concept. According to this rule, every simple image or speech recognition system seems to qualify, regardless of the scope of its capabilities; however, this is a minority position in the Generative AI systems literature[89,90].

Second, a smaller definition would not prevent further difficulties. Large AI models are so versatile that most providers will not be able to utilise the exception in Art. 4(c) of the AI Act: by excluding all high-risk uses, they would not be acting in good faith, as they would have to be aware that the system, once released, will likely be used for at least one high-risk application. For instance, language models can be utilised to summarise or evaluate medical patient data, as well as student, employment, credit, and insurance applications. In the absence of a technically verifiable exclusion of misuse, generative AIs will be categorised as high-risk systems under the proposed clause. This, however, necessitates that they comply with the high-risk duties, including the implementation of a comprehensive risk management system, as stipulated in Article 9 of the AI Act. Given the variety of generative AIs, setting up such a system appears nearly impossible. This appears not just nearly excessively expensive but also improbable.

Finally, the present regulations are anticipated to have substantial negative effects on the competitive environment around generative AIs. In fact, all companies, regardless of size, creating generative AIs and placing them on the market will be subject to the same strict high-risk requirements and liability risks under the new product liability framework[91]. Given the complexity of complying with the AI Act's standards, it seems likely that only major companies with substantial pockets (such as Google and Microsoft) will be able to fund the production of an AI Act-compliant system. Compliance is going to be too expensive especially for open-source developers. Consequently, the AI Act may have the unintended effect of increasing anticompetitive market concentration in generative AI development. For instance, similar impacts regarding the GDPR have also been proven[92].

It seems therefore clear that the uniquity of generative AI systems requires ad-hoc solutions in terms of regulation. Obviously, the above objections and criticism do not imply that generative AI should not be regulated at all. Nevertheless, we feel a fresh strategy is required. Scholars have remarked that regulatory focus should move to deployers and users, i.e., those calibrating generative AI for high-risk concrete applications and using them[86].

In this sense, unique legal definitions are needed to capture the important participants in the AI industry chain. This includes developers, deployers, professional and non-professional users, and output receivers. Such a sophisticated comprehension is required to assign regulatory responsibilities to certain actors and activities in the AI value chain. The basic strategy taken by the EU Council with the AI Act fails to address the large generative AI value chain's particularities.

4. Implementing AI in a smart city: The matter of fairness, privacy and transparency

In an urban smart city context, artificial intelligence technologies and solutions are already being used in a number of industries, including energy management, environmental monitoring, public safety, transportation and predictive maintenance[93].

Additionally, the environment for urban research has changed from being data-poor to data-rich. This means that a variety of sources, including sensors and cameras connected to buildings, factories, parks, roads, sidewalks and other urban features, can be used to synthesise heterogeneous real-time data. Artificial intelligence will in fact use source data from sensors, satellite imagery, and social media across space and time to produce outputs that enable more informed decisions on how to optimise urban operations[35].

Finally, the boundary between disciplines and urban applications has become blurred due to the increase in computing power and information technology. Collaboration between stakeholders and disciplines is often critical to effectively address complex urban challenges[94]. AI has the potential to revolutionise urban planning education and practice by providing planners with new tools to automate certain processes and make informed judgements[2]. However, ethical and regulatory challenges are still present and must be addressed in parallel to the deployment of AI technologies in Smart Contexts[3]. In particular, we find three main principles that a regulatory framework could base itself upon in order to balance inefficiencies derived from the inherent complexity of AI: fairness, privacy and transparency.

4.1. Fairness

The AI Act, whose preamble explicitly states that high-risk AI systems must be accompanied by instructions for use, including, where necessary, concise information on the risk of discrimination, was proposed by the EU in an effort to put the political position of fairness into practice. As we have seen, this has been done proactively. Others, however, have criticised the AI Act for not going far enough in reducing potential harm from bias in high-risk systems, pointing to the vague and non-committal terminology used in differential impact assessments and the lack of defined mechanisms for bias checks[95]. It is clear that a thorough understanding of AI fairness inspired by individual equality, proportionate systems and the right to redress is emerging, and interpretations will be limited by these aspects as more research is conducted to clarify these measurements. By comparison, the Chinese AI Ethics Principles also strongly emphasise the importance of fairness. Beyond these high-level concepts, however, the topic of AI fairness policies hasn't been thoroughly explored until recently[96].

Although there is a strong focus on consumer empowerment in policy documents, which can be seen as an implicit pursuit of these goals, there aren't many other sections dedicated to eliminating harmful bias. For example, according to the Draft Regulation on Recommendation Systems included in the Digital Services Act (and its Article 17), users should be able to disable recommendations and tools for selecting or deleting user labels used in algorithmic recommendation systems that focus on their personal characteristics. While these regulations have the potential to give consumers more power to challenge unfair judgements, as only the tech-savvy will be able to use them, they may instead lead to more unequal outcomes[69].

4.2. Privacy

From the AIA perspective, the Privacy is broken down into the "protection of the individual", which explains the GDPR references, and the technical privacy (i.e., cybersecurity and cybergovernance), which is referenced for high-risk system in article 15 of the Act[7].

Technical privacy can be brushed of easily in the EU context: multiple regulations rule the matter and provide ample and sufficient protection. One could have wished for a more detailed legal implementation of the current regulatory methods: for instance, the creation of a mandatory Data protection impact assessment. The need to conduct a Data Protection Impact Assessment may be triggered by the use of new technologies and the enhanced processing of data groups using artificial intelligence[97]. In combination with another activity from the Guidelines on Data Protection Impact Assessments, such as systematic monitoring, the use of cutting-edge technology or the generation of biometric or generic information also requires an organisation in smart cities to conduct an assessment. In order to examine specific characteristics of artificial intelligence, such as robustness, efficiency, transparency, bias minimisation and liability, an enhanced privacy and data protection impact assessment is strongly recommended.

When it comes to privacy, however, the "protection of the individual" perspective is not enough to cover the full problematics of the smart city. There are important factors that need to be taken into account in order to address the issues of privacy and artificial intelligence, especially in smart cities. To ensure that institutions are moving towards sound data management, privacy should be improved by default or design in smart cities[6], and not as an afterthought as it is currently in the AIA. Mandatory structures should include:

- Data minimisation techniques are used in artificial intelligence execution techniques to ensure that only relevant data is collected, processed and retained by the system for intelligence according to the defined purpose.
- Purpose limitation strategies such as isolating categories of data are another option to ensure that data sets are used for their intended purpose.
- Security techniques such as pseudonymisation or anonymisation of probable information, implementation of access controls, encryption and audit logs are the final method of implementing artificial intelligence.

Ensuring transparency (see section 4.3) could also help us overcome obstacles related to artificial intelligence and privacy. Institutions seeking to use artificial intelligence in smart city technologies should closely monitor transparency obligations to address the GDPR's requirement for lawful, equal and transparent processing and the Ethics Guidelines for Trustworthy Artificial Intelligence's transparency concerns[98]. Therefore, organisations may need to develop a layered model that includes symbols and marks around the city.

Current administrative privacy notices can be revised to achieve a higher level of transparency. A legal justification for processing, such as public interest, should be at the heart of the review. Furthermore, organisations in smart cities can more effectively adopt and implement internal policies to demonstrate their compliance with the GDPR. There is a need to establish guidelines and accountability for communicating decisions facilitated by artificial intelligence to people[99].

4.3. Transparency

Knowledge is not created in a vacuum, but through critical and transparent discourse within the epistemic conditions of contemporary social organisation[100]. While openness fosters creativity, encourages criticism and guards against cognitive and other biases in society, it also ensures responsiveness, efficiency and accountability in government, which promotes effective governance[101]. Standard regulatory tools to create openness and thus to foster the growth of knowledge include individual access to information rights, mandatory disclosure rules or investigatory authorities granted to public authorities. The opacity of AI will ultimately determine whether these rights and obligations, collectively referred to as "access to information regulation", can increase transparency in the case of AI[102]. Given the normative positions of those who would be adversely affected by transparency rules, it is also important to consider whether such rules can be created in a necessary and proportionate manner[102]. The capacity of individual stakeholders to process the knowledge gained through such regulation should be taken into account by regulators when deciding whether and to what extent to regulate access to information for AI.

Unlike the two previous goals which are not met, we can affirm that the AIA has a decent protection of transparency (in high-risk AI cases): first of all, it asks that transparency should be implemented by design (art. 13(1)), should include proper instructions according to a pre-determined template (13(2/3)), but also include proper human review (14), which must be allowed to answer problematic cases (Article 12).

The treatment of digital technologies, including the usage of AI, must be universally understandable and manageable for users as well as for supervisory authorities and the general public[103]. In this sense, establishing trust is a precondition for establishing accountability and, in some situations, culpability. Strict legal restrictions can be avoided by carefully selecting where to incorporate, by moving activities to other parts of the group if doing so weakens the requirements that must be observed. Again, the AIA manages to convert that problem with a territorial application of the law to the whole EU (and adds a duty to inform and cooperate with the authorities, Article 22–23): one should hope its application will happen uniformly.

Despite the fact that the digital transformation has opened up previously virtually inaccessible spaces for the generation, capture, and exploitation of information, technology design can still restrict access to the methods used and the outcomes. Collaboration in the creation of hardware and various program components can also lead to a lack of transparency. This is especially true when there is a lack of understanding of the "building blocks" originating from the other actors engaged and how these parts work.

Although the black-box nature of information technology systems can be bypassed, such as through reverse engineering, doing so typically requires a high level of skill and the application of intricate techniques. Regulation, additionally, may become a barrier to transparency in situations when algorithms are recognized as trade secrets or as government secrets. This is, so far, the only element which the AIA regulation fails to address properly: what about state secrets?

5. Conclusion

The advancement of artificial intelligence technology has the potential to fundamentally alter the nature and scope of the law. However, the legal community must make sure that technology is used ethically and in accordance with the relevant rules. In order to provide oversight and guarantee that legal decisions made by artificial intelligence are fair, just, and in accordance with the law, this necessitates the development of new laws and regulations.

In order for the legal profession to decide on the proper application of artificial intelligence in legal practice, it is crucial to ensure that its members are properly educated on technology and its ramifications. Integrating AI into the judicial system opens up a number of novel opportunities for enhancing effectiveness, accuracy, and fairness. Governments ought to consider enacting rules and legislation to ensure that AI-based technologies are applied morally and responsibly. In order to identify and manage any potential dangers that may result from the usage of AI technology, legal professionals should also be knowledgeable about its use and effects.

Regulators and legislators must move swiftly in all sectors to stay up with the unrestrained dynamics of emerging, constantly evolving AI technology. In order to preserve the decorum of online discourses and to establish a fair playing field for the creation and application of the next generation of AI models, both within the EU and outside of it, updated regulation is required.

Finally, more investigation is required to assess the potential legal repercussions of AI and to create best practices for its ethical and responsible application. AI has the potential to be a significant instrument for preserving the effectiveness and justice of the legal system when used properly.

Conflicts of interest

The author declares no conflict of interest.

Notes

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] *"(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm."*

[3] *"(d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives: (i) the targeted search for specific potential victims of crime, including missing children; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack."*

[4] To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

[5] For high-risk AI usage—*"High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title"*.

[6] *"If there are many, they must be as many as they are and neither more nor less than that. But if they are as many as they are, they would be limited. If there are many, things that are are unlimited. For there are always others between the things that are, and again others between those, and so the things that are are unlimited."* From Simplicius: On Aristotle's Physics, 140.29.

[7] Article 15 Accuracy, robustness and cybersecurity—High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle.

References

1. Yigitcanlar T, Desouza K, Butler L, Roozkhosh F. Contributions and Risks of Artificial Intelligence (AI) in Building Smarter Cities: Insights from a Systematic Review of the Literature. Energies. 2020;13(6):1473.

doi:10.3390/en13061473

2. Sanchez TW, Shumway H, Gordner T, Lim T. The prospects of artificial intelligence in urban planning. International Journal of Urban Sciences. 2022;27(2):179-194. doi:10.1080/12265934.2022.2102538
3. Ahmad K, Maabreh M, Ghaly M, et al. Developing future human-centered smart cities: Critical analysis of smart city security, Data management, and Ethical challenges. Computer Science Review. 2022;43:100452. doi:10.1016/j.cosrev.2021.100452
4. Rani S, Kataria A, Chauhan M, et al. Security and Privacy Challenges in the Deployment of Cyber-Physical Systems in Smart City Applications: State-of-Art Work. Materials Today: Proceedings. 2022;62:4671-4676. doi:10.1016/j.matpr.2022.03.123
5. André Q, Carmon Z, Wertenbroch K, et al. Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data. Cust Need and Solut. 2017;5(1-2):28-37. doi:10.1007/s40547-017-0085-8
6. Fabrègue BFG, Bogoni A. Privacy and Security Concerns in the Smart City. Smart Cities. 2023;6(1):586-613. doi:10.3390/smartcities6010027
7. Ebers M, Hoch VRS, Rosenkranz F, et al. The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). J. 2021;4(4):589-603. doi:10.3390/j4040043
8. Sharif RA, Pokharel S. Smart City Dimensions and Associated Risks: Review of literature. Sustainable Cities and Society. 2022;77:103542. doi:10.1016/j.scs.2021.103542
9. Allam Z, Dhunny ZA. On big data, artificial intelligence and smart cities. Cities. 2019;89:80-91. doi:10.1016/j.cities.2019.01.032
10. Khan S. Barriers of big data analytics for smart cities development: A context of emerging economies. International Journal of Management Science and Engineering Management. 2021;17(2):123-131. doi:10.1080/17509653.2021.1997662
11. Bharadiya J. Artificial Intelligence in Transportation Systems A Critical Review. AJCE. 2023;6(1):34-45. doi:10.47672/ajce.1487
12. Salama R, Al-Turjman F, Culmone R. AI-Powered Drone to Address Smart City Security Issues. In: Barolli L (editor). Proceedings of the Advanced Information Networking and Applications. Springer International Publishing: Cham; 2023. pp. 292–300.
13. Cath C, Wachter S, Mittelstadt B, et al. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. Sci Eng Ethics. 2017. doi:10.1007/s11948-017-9901-7
14. Ulnicane I, Knight W, Leach T, et al. Framing governance for a contested emerging technology: Insights from AI policy. Policy and Society. 2020;40(2):158-177. doi:10.1080/14494035.2020.1855800
15. Vesnic-Alujevic L, Nascimento S, Pólvora A. Societal and ethical impacts of artificial intelligence: Critical notes on European policy frameworks. Telecommunications Policy. 2020;44(6):101961. doi:10.1016/j.telpol.2020.101961
16. Organisation for Economic. Co-operation and Development AI Policy and National Strategies. OECD; 2021.
17. Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. Nat Mach Intell. 2019;1(9):389-399. doi:10.1038/s42256-019-0088-2
18. European Commission. Artificial Intelligence for Europe. European Commission; 2018.
19. Marcus G, Davis E. Rebooting AI: Building Artificial Intelligence We Can Trust. Pantheon Books: USA; 2019.
20. Dyrhauge H. EU transport policy at a crossroads. The Routledge Handbook of European Integrations. 2022;208-219. doi:10.4324/9780429262081-16
21. Karampekios N. Iraklis Oikonomou Defence-Industrial Consolidation as a Precondition for EU Military Integration. In: The Routledge Handbook of European Integrations. Routledge; 2021.
22. James Manyika. 10 Imperatives for Europe in the Age of AI and Automation. McKinsey Global Institute; 2017.
23. European Commission. Whitepaper on Artificial Intelligence—A European Approach to Excellence and Trust. European Commission; 2020.
24. European Commission. Coordinated Plan on Artificial Intelligence. European Commission; 2018.
25. Schwemer SF, Tomada L, Pasini T. Legal AI Systems in the EU's Proposed Artificial Intelligence Act 2021. doi: 10.31235/osf.io/kpz5t
26. Schuett J. Defining the scope of AI regulations. Law, Innovation and Technology. 2023;15(1):60-82. doi:10.1080/17579961.2023.2184135
27. Tamanaha BZ. On the Rule of Law: History, Politics, Theory. Cambridge University Press: Cambridge; 2004.
28. Golding D. Precautionary Principle. International Encyclopedia of the Social & Behavioral Sciences. 2001:11961-11963. doi:10.1016/b0-08-043076-7/04163-2
29. Xue L, Pang Z. Ethical governance of artificial intelligence: An integrated analytical framework. Journal of Digital Economy. 2022;1(1):44-52. doi:10.1016/j.jdec.2022.08.003
30. Huscroft G, Miller BW, Webber G. Proportionality and the Rule of Law. Cambridge University Press; 2014. doi:10.1017/cbo9781107565272
31. McCarthy J. What Is Artificial Intelligence? Available online: http://www-formal.stanford.edu/jmc/whatisai/ (accessed on 23 May 2023).

32. Russel S, Norvig P. Artificial Intelligence: A Modern Approach. Pearson Education: New Jersey; 2021.
33. Copeland BJ. Artificial Intelligence (AI). Available online: https://www.britannica.com/technology/artificial-intelligence (accessed on 23 May 2023).
34. Chowdhary KR. Fundamentals of Artificial Intelligence, 1st ed. Springer: New Delhi; 2020.
35. Ye X, Du J, Han Y, et al. Developing Human-Centered Urban Digital Twins for Community Infrastructure Resilience: A Research Agenda. Journal of Planning Literature. 2022;38(2):187-199. doi:10.1177/08854122221137861
36. Kukka H, Foth M, Dey AK. Transdisciplinary approaches to urban computing. International Journal of Human-Computer Studies. 2015;81:1-3. doi:10.1016/j.ijhcs.2015.05.003
37. Korteling JE, van de Boer-Visschedijk GC, Blankendaal RAM, et al. Human- versus Artificial Intelligence. Front Artif Intell. 2021;4. doi:10.3389/frai.2021.622364
38. Misselhorn C. Grundfragen Der Maschinenethik. Reclam, Philipp, jun. GmbH, Verlag; 2018.
39. Duan Y, Edwards JS, Dwivedi YK. Artificial intelligence for decision making in the era of Big Data—Evolution, challenges and research agenda. International Journal of Information Management. 2019;48:63-71. doi:10.1016/j.ijinfomgt.2019.01.021
40. Dennehy D, Griva A, Pouloudi N, et al. Artificial intelligence for decision-making and the future of work. International Journal of Information Management. 2023;69:102574. doi:10.1016/j.ijinfomgt.2022.102574
41. Gardner HE. Multiple Intelligences: The Theory In Practice. A Reader; Basic Books; 1993.
42. March JG. Rationality, foolishness, and adaptive intelligence. Strategic Management Journal. 2006;27(3):201-214. doi:10.1002/smj.515
43. Mölders M. Legal Algorithms and Solutionism: Reflections on Two Recidivism Scores. SCRIPT. 2021;18(1):57-82. doi:10.2966/scrip.180121.57
44. Ehsani S, Glauner P, Plugmann P, Thieringer FM. The Future Circle of Healthcare. Springer International Publishing; 2022. doi:10.1007/978-3-030-99838-7
45. Svantesson D. The European Union Artificial Intelligence Act: Potential implications for Australia. Alternative Law Journal. 2021;47(1):4-9. doi:10.1177/1037969x211052339
46. European Commission. Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth. European Commission; 2010.
47. European Commission. Joint Research Centre. Artificial Intelligence: A European Perspective. Publications Office; 2018. doi:10.2760/11251
48. Boucher P. Artificial Intelligence: How Does It Work, Why Does It Matter, and What Can We Do about It? European Parliament; 2020.
49. European Group on Ethics in Science and New Technologies (EGE) Statement on Artificial Intelligence. Robotics and 'Autonomous' Systems. European Commission: Brussels; 2018.
50. European Economic and Social Committee. Artificial Intelligence—The Consequences of Artificial Intelligence on the (Digital) Single Market, Production, Consumption, Employment and Society. EESC; 2017.
51. European Commission. AI Policy Seminar: Towards an EU Strategic Plan for AI. Digital Transformation Monitor; 2017.
52. Ryan L. European Integration, the European Research Area and European Research Infrastructures. In: The Routledge Handbook of European Integrations. Routledge; 2021.
53. European Parliament. Resolution with Recommendations to the Commission on Civil Law Rules on Robotics. European Parliament; 2017.
54. High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI; Shaping Europe's digital future. European Commission; 2019.
55. European Commission. Fostering a European Approach to Artificial Intelligence. European Commission; 2021.
56. European Commission. Artificial Intelligence Act Proposal. European Commission; 2021.
57. European Data Protection Board. EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). EDPB; 2021.
58. European Central Bank. Opinion of the European Central Bank on a Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence. ECB; 2021.
59. European Commission. AI Liability Directive Proposal. European Commission; 2021.
60. European Council. Artificial Intelligence Act: Council Calls for Promoting Safe AI That Respects Fundamental Rights. Available online: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/ (accessed on 25 May 2023).
61. IMCO. LIBE Draft Compromise Amendments on the Artificial Intelligence Act. European Parliament; 2023.
62. European Data Protection Supervisor. Artificial Intelligence Act: A Welcomed Initiative, but Ban on Remote Biometric Identification in Public Space Is Necessary. Available online: https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative (accessed on 25 May 2023).
63. European Commission. Digital Services Act Proposal. European Commission; 2020.

64. European Commission. Digital Markets Act Proposal. European Commission; 2020.
65. De Gregorio G. The rise of digital constitutionalism in the European Union. International Journal of Constitutional Law. 2021;19(1):41-70. doi:10.1093/icon/moab001
66. European Commission. Data Governance Act Proposal. European Commission; 2020.
67. European Commission. Regulation on the European Health Data Space Proposal. European Commission; 2022.
68. Roberts H, Cowls J, Hine E, et al. Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. The Information Society. 2022;39(2):79-97. doi:10.1080/01972243.2022.2124565
69. Roberts H, Cowls J, Hine E, et al. Achieving a 'Good AI Society': Comparing the Aims and Progress of the EU and the US. Sci Eng Ethics. 2021;27(6). doi:10.1007/s11948-021-00340-7
70. Barrett C. Are the EU GDPR and the California CCPA Becoming the De Facto Global Standards for Data Privacy and Protection? Scitech Lawyer. 2019;15:24-29.
71. European Commission. High Representative of the Union for Foreign Affairs and Security Policy Joint Communication: A New EU-US Agenda for Global Change. European Commission; 2020.
72. Fabrègue BFG, Bogoni A. Nudging: A double-edged sword in the era of Big Data. In: Proceedings of 2023 8th International Conference on Smart and Sustainable Technologies (SpliTech); 2023. doi:10.23919/splitech58164.2023.10192971
73. Karpa D, Klarl T, Rochlitz M. Artificial Intelligence, Surveillance, and Big Data. In: Hornuf L (editor). Diginomics Research Perspectives: The Role of Digitalization in Business and Society. Advanced Studies in Diginomics and Digitalization. Springer International Publishing: Cham; 2022. pp. 145–172.
74. Leibold J. Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement. Journal of Contemporary China. 2019;29(121):46-60. doi:10.1080/10670564.2019.1621529
75. Zhang Y, Hua J, Adu Gyamfi B, Shaw R. Artificial Intelligence and Its Importance in Post-COVID-19 China. In: Considerations for a Post-COVID-19 Technology and Innovation Ecosystem in China. Disaster Risk Reduction. Springer: Singapore; 2022. pp. 115–125.
76. Veale M, Zuiderveen Borgesius F. Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International. 2021;22(4):97-112. doi:10.9785/cri-2021-220402
77. Smuha NA, Ahmed-Rengers E, Harkens A, et al. How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act. SSRN Journal. 2021. doi:10.2139/ssrn.3899991
78. Enarsson T, Enqvist L, Naarttijärvi M. Approaching the human in the loop—Legal perspectives on hybrid human/algorithmic decision-making in three contexts. Information & Communications Technology Law. 2021;31(1):123-153. doi:10.1080/13600834.2021.1958860
79. Peters B. Aspects of Human Rights Interpretation by the UN Treaty Bodies. In: UN Human Rights Treaty Bodies. Cambridge University Press; 2011.
80. Yeung K. Why Worry about Decision-Making by Machine? In: Algorithmic Regulation. Oxford University Press; 2019.
81. Glaese A, McAleese N, Trębacz M, et al. Improving alignment of dialogue agents via targeted human judgements. arXiv. 2022;arXiv:2209.14375. doi:10.48550/ARXIV.2209.14375
82. Meskó B, Topol EJ. The imperative for regulatory oversight of large language models (or generative AI) in healthcare. npj Digit Med. 2023;6(1). doi:10.1038/s41746-023-00873-0
83. Aung YYM, Wong DCS, Ting DSW. The promise of artificial intelligence: A review of the opportunities and challenges of artificial intelligence in healthcare. British Medical Bulletin. 2021;139(1):4-15. doi:10.1093/bmb/ldab016
84. Mirsky Y, Demontis A, Kotak J, et al. The Threat of Offensive AI to Organizations. Computers & Security. 2023;124:103006. doi:10.1016/j.cose.2022.103006
85. Marcus G. A Skeptical Take on the A.I. Revolution. N. Y. Times; 2023.
86. Hacker P. Understanding and Regulating ChatGPT, and Other Large Generative AI Models. Verfassungsblog: On Matters Constitutional. 2023. doi:10.17176/20230120-220055-0
87. Edwards L. Regulating AI in Europe: Four Problems and Four Solutions. Ada Lovelace Institute; 2022.
88. Brown TB, Mann B, Ryder N, et al. Language Models Are Few-Shot Learners. ArXiv. 2020.
89. Gutierrez CI, Aguirre A, Uuk R, et al. A Proposal for a Definition of General Purpose Artificial Intelligence Systems. SSRN Journal. 2022. doi:10.2139/ssrn.4238951
90. Bennett CC, Hauser K. Artificial intelligence framework for simulating clinical decision-making: A Markov decision process approach. Artificial Intelligence in Medicine. 2013;57(1):9-19. doi:10.1016/j.artmed.2012.12.003
91. Hacker P. The European AI Liability Directives—Critique of a Half-Hearted Approach and Lessons for the Future. SSRN Journal. 2022. doi:10.2139/ssrn.4279796
92. Geradin D, Karanikioti T, Katsifis D. GDPR Myopia: How a well-intended regulation ended up favouring large online platforms—The case of ad tech. European Competition Journal. 2020;17(1):47-92. doi:10.1080/17441056.2020.1848059

93. Jabbar MA, Tiwari S, Ortiz-Rodriguez F. Smart Urban Computing Applications. CRC Press; 2023.
94. Portal L, Fabregue B. Establishing Participative Smart Cities: Theory and Practice. Smart Cities Reg. Dev. SCRD J. 2022;6:43-62. doi:10.25019/scrd.v6i2.128
95. MacCarthy M. Kenneth Propp Machines Learn That Brussels Writes the Rules: The EU's New AI Regulation. Lawfare; 2021.
96. Wu W, Huang T, Gong K. Ethical Principles and Governance Technology Development of AI in China. Engineering. 2020;6(3):302-309. doi:10.1016/j.eng.2019.12.015
97. Braun T, Fung BCM, Iqbal F, Shah B. Security and privacy challenges in smart cities. Sustainable Cities and Society. 2018;39:499-507. doi:10.1016/j.scs.2018.02.039
98. Yanisky-Ravid S, Sean K. Hallisey "Equality and Privacy by Design": A New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes. Fordham Urban Law J. 2019;46:428.
99. Vinod Kumar TM. E-Governance for Smart Cities. Springer Singapore. 2015. doi:10.1007/978-981-287-287-6
100. Merton R. Social Theory and Social Structure. Macmillan: New York; 1968.
101. Hood C, Heald D. Transparency: The Key to Better Governance. Proceedings of the British Academy. Oxford University Press; 2006.
102. Wischmeyer T. Artificial Intelligence and Transparency: Opening the Black Box. In: Wischmeyer T, Rademacher T (editors). Regulating Artificial Intelligence. Springer International Publishing: Cham; 2020. pp. 75–101.
103. Nemitz PF. Constitutional Democracy and Technology in the age of Artificial Intelligence. SSRN Journal. 2018. doi:10.2139/ssrn.3234336