

The risks associated with generative AI apps in the European Artificial Intelligence Act (AIA)

Maryna Vahabava^{1,2}

¹Post Doc Scuola Superiore Universitaria Sant'Anna of Pisa

²This work is supported by the European Union under the scheme HORIZON-INFRA-2021-DEV-02-01 – Preparatory phase of new ESFRI research infrastructure projects, Grant Agreement n.101079043, “SoBigData RI PPP: SoBigData RI Preparatory Phase Project”

Abstract

Artificial Intelligence-based technologies offer new development opportunities in traditional economic sectors and, at the same time, raise many legal, ethical, and technological issues. This article attempts to analyze the most important innovations of the EU's Artificial Intelligence Act (AIA), based on the risk management approach. In this context, particular role is presented by Generative Artificial Intelligence, as ChatGPT, case observed by the Italian national Data Protection Authority.

Keywords

Artificial Intelligence Act (AAI), Artificial Intelligence (AI), Generative Artificial Intelligence (GPAI), ChatGPT, Italian Data Protection Authority

1. Introduction

New technologies have developed rapidly to become an integral part of people's social, working, and organizational lives¹. The spread of the global Covid-19 pandemic has accelerated this process in areas such as education, social interactions, business organizational models, health protection and rights to social cooperation. For these reasons, the role of artificial intelligence (AI) has become central to the lives of citizens, companies, and institutions. New technologies based on AI offer new development opportunities in traditional economic sectors and, at the same time, raise many legal, ethical, and technological issues. This article attempts to analyze the most important innovations of the EU's Artificial Intelligence Act (AIA), with particular attention to legal, technical, and ethical issues. The act is of particular importance considering that it represents a first worldwide attempt to regulate AI based on the risk management approach related to the application of systems based on the new technology². In this context,


HHAI-WS 2023: Workshops at the Second International Conference on Hybrid Human-Artificial Intelligence (HHAI), June 26–27, 2023, Munich, Germany

✉ Maryna.Vahabava@santannapisa.it (M. Vahabava)

🆔 0000-0002-4746-6436 (M. Vahabava)



© 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

¹McCarthy, M. L. Minsky, N. Rochester, C. E. Shannon, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, *AI Mag.* 27.4 (2006).

²M. Bussani, L'Unione Europea Al Grande Passo: Verso Una Regolazione Di Mercati E Servizi Digitali, *Quad. Costituzionali* (2021) 224–227; R. J. Neuwirth, *The EU Artificial Intelligence Act*. Milton: Taylor Francis Group, Law Emerg. Technol. Milton: Taylor & Francis Group (2022).

particular role is presented by software called Generative Artificial Intelligence. These new tools are not limited to providing information to users based on certain input criteria, but they learn independently from previous experiences and evolve in a surprising way thanks to machine learning. The Generative Artificial Intelligence apps are a novelty that allows to automate some of the most important human actions: from writing literal and musical texts to the structuring of the strings of computer codes or medical surveillance. At the same time, these programs have important risk factors to consider, such as the incorrect use of user data collected, the veracity of the information provided, cybersecurity and others. These risks can be managed by the European AIA Regulation (AIA)³, which, with different techniques of approach, has the aim to protecting European citizens from the possible damage resulting from the use of Artificial Intelligence tools (including Generative Artificial Intelligence apps). A particular attention deserves the Italian ChatGPT case that has been subjected to the control by the national Data Protection Authority. This specific software, that allows to obtain the answers to the questions of users in various areas, including the legal sector, attracted the attention of the Italian Authority because of loss of personal data during the training phase of the algorithm that involved people participating. For this reason, the Italian Privacy Authority issued a measure in which it invited the American software developer company to provide clarification on the correct management of user data and compliance with European privacy rules. This is an important precedent for the development of artificial intelligence software and for computer companies located outside the European Union and for euro area users. To conclude the EU is trying to introduce regulations on the use of Artificial Intelligence systems in a more transparent and secure way. In particular, the Artificial Intelligence Act (AIA) is a law of the European Union that intends to regulate various aspects related to Artificial Intelligence (AI) that is about to be definitively approved by the European Parliament⁴. It is useful to analyze the most important innovations that will be introduced with the European Regulation, especially in relation to the Generative AI applications. The document aims to manage the risks involved and limit the misuse of software, but it does not seem to consider all the possible implications of generative AI. The software is an active and highly contested area of research and should be the subject of extensive consultation, including with civil society, researchers, and others, because it involves different risks and poses ethical questions . The Regulation should take into consideration the specificities of software and provide legal protection for all phases of the development and implementation of Generative Purpose AI applications.

2. The main innovations which contain the Artificial Intelligence Act (AIA)

The Artificial Intelligence Act (AIA) deals with the definition of the concept of Artificial Intelligence (AI), listing the technologies that fall into this category for the purpose of applying

³N. Purtova, The law of everything. Broad concept of personal data and future of EU data protection law, *Law, Innov. Technol.* 10.1 (2018) 40–81.

⁴M. Ebers, V. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrotter, The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS), *Multidiscip. Sci. J.* 4 (2021) 589–603.

regulation. The Regulation contains a list of activities defined as high risk, capable of producing negative consequences in various respects and in different areas as well as a list of activities of AI banned in the European area⁵. Part of the AI Act is devoted to possible exceptions to the categories described above and the criteria for the flexible application of the Regulation are identified. The main aim is to protect the rights of citizens of the European Union (also in the sense of the category of consumers) from the possible risks of using the new technological tools of AI, with particular attention to businesses and the labor market⁶. It should not be overlooked that the new regulation aims to provide greater protection for the use of AI technologies to the most vulnerable people, such as children, the elderly and the disabled. For this reason, criteria are established to more clearly define which legitimate and lawless activities involve the use of artificial intelligence⁷. On the one hand, the European Union encourages and encourages the use of new technologies in order to ensure greater development and progress for citizens and businesses; on the other hand, attempts to regulate and manage the most important aspects and to identify and reduce the risks associated with the use of artificial intelligence systems⁸. Although the topic is not new to the debate, this Act is the first law in the world that regulates this technology in an organic⁹. In addition to the objectives described above, the AI Act aims to protect fundamental human rights. For all these reasons, the Act could become a model for other countries outside the European Union. One of the most discussed issues concerns the definition of Artificial Intelligence to apply the new rules¹⁰. The definition of artificial intelligence adopted in the Commission proposal of 21 April 2021 has been criticized, in the first place, by other bodies of the European Union. The European Economic and Social Committee ("EESC") in its opinion adopted on 22 September 2021, recommended to clarify the definition of AI by deleting Annex I. The latter lists the techniques and approaches by which software should be developed to fall within the definition of Artificial Intelligence¹¹. According to these reasons, the text has been amended and adapted. Instead, the Council of the European Union adopted a different approach in the first compromise text of 29 November 2021, more restrictive to ensure greater legal certainty¹². The most common criticism that has been made, even by some consumer associations, was that the Commission's definition included almost all software, making the scope of the Regulation too broad¹³. For these reasons, the definition in Article 3 of the proposed AIA Regulation of the artificial intelligence system has been completely modified to indicate the three characteristics that the software must have to be considered an artificial intelligence

⁵G. Resta, B. Carotti, G. Squeo, A. Simoncini, O. Pollicino, M. Libertini, G. Finocchiaro, L. Torchia, La Regolazione Digitale Nell'Unione Europea, Riv. Trimest. Dirit. Pubblico 4 (2022) 791

⁶*Ibidem*

⁷I. De Matos Pinto, The Draft AI Act: A Success Story of Strengthening Parliament's Right of Legislative Initiative?, ERA-Forum 22.4 (2021) 619–461.

⁸*Ibidem*

⁹R. J. Neuwirth, The EU Artificial Intelligence Act. Milton: Taylor Francis Group, Law Emerg. Technol. Milton: Taylor Francis Group (2022)

¹⁰*Ibidem*

¹¹D. Svantesson, The European Union 'Artificial Intelligence Act': Potential Implications for Australia, Altern. Law J. 47.1 (2022).

¹²I. De Matos Pinto, The Draft AI Act: A Success Story of Strengthening Parliament's Right of Legislative Initiative?, ERA-Forum 22.4 (2021) 619–461.

¹³D. Svantesson, The European Union 'Artificial Intelligence Act': Potential Implications for Australia, Altern. Law J. 47.1 (2022).

system. According to the new definition, an artificial intelligence system is a system that: (i) receives data and inputs from devices and/or humans; (ii) deduces how to achieve a set of human-defined goals using learning, the reasoning or modelling implemented with the techniques and approaches listed in Annex I, and (iii) generates results in the form of content (generative AI systems), predictions, recommendations or decisions, which influence the environments with which it interacts¹⁴. This definition, on the one hand, was welcomed by the high-level group of experts on artificial intelligence, since it is more precise and considerably restricts the scope of the Regulation. On the other hand, has been criticized by associations that defend fundamental rights (such as Algorithmwatch and AccessNow). For the latter, it is still necessary to develop a broad definition of artificial intelligence to better protect fundamental rights. Another aspect that has to be considered is the transparency regarding the functioning of algorithms underlying AI systems. This issue not only concerns the security of the data management of citizens and businesses, but also prevents a legality check by the state authorities. Finally, a further issue closely linked to what has just been said is of an ethical nature: respect for human rights on the part of the legal rules laid down by the individual state systems. In this perspective, AIA intends to prohibit "social scoring" practices, that is, the allocation of social scores to individuals as well as their monitoring and discrimination based on personal score. Social control systems through AI scores and use will be banned in the EU¹⁵. What is still controversial is biometric control via real-time video surveillance enhanced by AI systems. Such use poses serious risks of violation of the fundamental rights of individuals if the instrument is used for non-consensual or invasive purposes in the personal sphere¹⁶. Another problem concerns the technical functioning of the algorithms underlying the Artificial Intelligence because some of them can evolve and learn from their actions and from users inputs. Software learning techniques include a part of training that is carried out with the help of people. Such techniques can lead to the risks of using personal data also in a wrong way, if they are not regulated and, where necessary, limited or prohibited. Several Artificial Intelligence-based technologies are developed by private companies with registered offices outside the Europe Union, although they are in fact used by many European users. This makes it difficult to identify the applicable forum in case of possible disputes. The issue of jurisdiction and the identification of applicable laws is topical. The AI Act aims to regulate this aspect to better protect the rights of EU citizens. The risk of misinformation arising from the use of software based on AI tools should be considered. Some applications allow to obtain information based on user requests, such as ChatGPT. However, the information given is not always true and up-to-date due to the technical structure of the software and this can cause damages. The Artificial Intelligence Act also aims to manage this aspect to better protect users by requiring developers to manage the risk appropriately¹⁷. The integration of the AI Act with respect to the protection of privacy should be considered, as the possible misuse of data and/or applications can have an important impact on the habits of citizens and businesses. For this reason, it is necessary to ensure the transparent use of data

¹⁴ *Ibidem*

¹⁵ H. Ruschmeier, AI as a Challenge for Legal Regulation – the Scope of Application of the Artificial Intelligence Act Proposal, ERA-Forum 23.3 (2023) 361–36.

¹⁶ *Ibidem*

¹⁷ H. Ruschmeier, AI as a Challenge for Legal Regulation – the Scope of Application of the Artificial Intelligence Act Proposal, ERA-Forum 23.3 (2023) 361–36.

and that users can learn about the operational mechanisms of the algorithms used by AI. The objective of the Artificial Intelligence Act is to impose rules that make the procedures for the use and collection of AI data in the EU transparent, even if they are developed outside the territory of the Union. This is because a large part of the systems is developed in the United States of America and other non-EU countries. To address the problems described above, the Artificial Intelligence Act tends to have three main strategies in its approach, developing a person-centered mindset. The European regulation will oblige companies to develop and apply Artificial Intelligence technologies with user and human rights in mind. Companies will have to demonstrate that their AI-based products and services do not affect people's rights, from freedom to non-discrimination, to the right to access to information. Other important aspects of regulation are safety and reliability. Artificial Intelligence systems will need to meet precise safety and reliability standards before they can be marketed, to minimize errors and the impact they can have on critical infrastructure. Finally, Artificial Intelligence Act's risk management strategy is based on risk classification. AI applications will be classified according to the level of danger to people and more or less stringent requirements will apply at each level¹⁸.

3. What are generative Artificial Intelligence apps and which risk involving

Generative artificial intelligence models (or generative AI app/chat) are software that produce text and images, such as blog posts, program codes, poems, artwork, and more. The software, which is based on artificial intelligence systems, uses complex machine learning models to predict the next word based on sequences of previous words or the next image based on words describing previous images¹⁹. Generative AI, more generally, represents any type of automated process that uses algorithms to produce, manipulate or synthesize data, often in the form of images or human-readable text. It's called generative purpose because AI creates something that didn't exist before²⁰. This is what differentiates it from discriminatory AI, which makes distinctions between different types of inputs. This application uses machine learning to process a huge amount of visual or textual data in order to determine which are most likely to appear true close to the others in a given contest. Generative AI programming is based on algorithms that can answer to external requests or inputs from users²¹. The software creates its results by evaluating a huge corpus of data on which it has been trained, and then answering to requests with something within the scope of the probability determined by that corpus. The process by which models are developed to fit all this data is called training. There are a couple of basic techniques for different types of models. Some software uses the so-called transformer model that works in such a way as to place words in a context giving them a precise meaning. This means that the system takes into account the position of one word with respect to the other

¹⁸J. Mökander, J. Prathm, D. S. Watson, L. Floridi, The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?, *Minds Mach.* 32.4 (2022) 751–758.

¹⁹F. Casarosa, Cybersecurity Certification of Artificial Intelligence: A missed Opportunity to Coordinate between the Artificial Intelligence Act and the Cybersecurity Act, *Int. Cybersecur. Law Rev.* 3.1 (2022) 115–130.

²⁰*Ibidem*

²¹J. Mökander, J. Prathm, D. S. Watson, L. Floridi, The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?, *Minds Mach.* 32.4 (2022) 751–758.

and the more general discourse in which the individual sentences thus formed are placed. A check is made of how one word can be related to another, also determining the probability of one being close to the other. These "transformers" are performed unsupervised on a vast corpus of natural language texts in a process called pretraining, before being developed by humans interacting with the model. Another technique used to train models is the opposing generative network (GAN). In this technique, there are two competing algorithms. One generates text or images based on probabilities derived from a large data set; the other is a discriminatory AI, which has been trained by humans to assess whether the output is real or generated by AI. Generative AI repeatedly tries to "deceive" discriminative AI, automatically adapting to help succeed. It should be noted that although human intervention is expected in the training process, most of both learning and adaptation is done in automatic mode. This can create problems, such as errors and answers that are likely or unlikely. One of the examples of this innovative technological tool is the ChatGPT, that use transformer model technique of software training, which will be discussed in the next paragraph. There are also other generative AI tools that allow you to perform different tasks using AI, which are usually done by humans. For example, the Chatsonic, a chatbot specialized in the search of linguistic data and images, voices and sounds. Chinchilla of Deep Mind is, instead, a model of AI specialized in the creation of content, usable to describe products inserted in e-commerce sites, or for the writing of articles of sites and blogs. There is software called Rytr that promises to write novels based on some indications provided in input by users such as the theme, the length, and other variables. To do this, is necessary only select the language, tone, and format and operate the command for the AI to write the novel text²². The company Meta has developed Make-a-Video, a tool that allows to generate videos based on certain text commands that must be entered by the user. Another area of application is computer encoding. The same ChatGPT allows to do "coding", but there is also other software, such as the GitHub Copilot, which helps software developers in writing or correcting strings of code. Generative AI also helps in the composition of musical works. There are right now programs that can create simple musical compositions as well as those more elaborate or dedicated to the creation of soundtracks. The programs mentioned above are based on deep learning architectures with algorithms that are formed through more or less extensive databases, which can relate to the discography of artists or the production of a certain kind of music. There are many innovations brought by new tools, such as generative AI chat, but we must not overlook the critical aspects. First of all, the protection of privacy with regard to the usage of generative Ai chats utilising large amounts of data in order to use the algorithm behind the software. In that context, the compatibility of the technological instrument with the rules of the European Privacy Regulation should be assessed. For example, you need to consider using personal images or videos to train and develop the algorithm or spreading fake news. Such situations can, if not managed in a fair and transparent way, create abuses that today cannot be tolerated. Another issue of fundamental importance is cybersecurity to prevent possible fraud and misuse to the detriment of citizens and businesses. Cybersecurity is one of the pillars necessary for the proper development of new technologies, such as the one in

²²T. İnce, Salih, European Union Law and Mitigation of Artificial Intelligence-Related Discrimination Risks in the Private Sector: With Special Focus on the Proposed Artificial Intelligence Act, *Ann. Fac. Droit D'Istanbul* 71 (2022) 265–307.

comment. Some solutions have already been developed to address the issues identified. This is the case of platforms, such as Aindo, that deal with "data curation" throughout the value chain. That is, from the structuring of real information to the creation of synthetic digital data and up to the use of these for predictive analysis. Such solutions, used in the medical and financial fields, can be extended to other sectors and fields that form the basis of AI systems computing²³.

4. ChatGPT case to the attention of the Italian Data Protection Authority

The deactivation of ChatGPT (Chat Generative Pretrained Transformer) in Italy, an artificial intelligence system able to provide answers to the questions asked by users, has aroused curiosity and interest in the legal field. In fact, with a recent measure (number 112 of 30 March 2023) of the Authority for the Protection of Personal Data, the American company OpenAI, which manages the program, was asked to provide some clarification on the processing of personal data, suspected violations of the European Privacy Regulation (GDPR)²⁴. The decision of the Italian Authority comes because of the loss of personal data suffered by the program on 20 March of the current years regarding user conversations, including information on the payment methods of certain subscription services. The company had to respond within twenty days of the decision; however, it preferred to temporarily suspend access to the service in Italy. In this way it was not the Guarantor who blocked access, but the company itself spontaneously closed access to Italian users. The reason of this choice is not clear, perhaps it was dictated by the desire to avoid sanctions in case of confirmation of suspected irregularities. The Italian case is interesting because, given the European origin of the rules on data protection, it could represent an interesting precedent for the whole European Union. The risk is that other Member States of the Union can also act like Italy and, consequently, arrive at the ChatGPT access block throughout the EU. It follows that the software company cannot underestimate the issue and, where necessary, must adapt to compliance with European data protection rules if it is to operate on the euro area market. To fully understand the decision of the Italian Privacy Authority it is useful to briefly analyze how ChatGPT works. It is a chatbot, or software, based on algorithms that, thanks to the evolved artificial intelligence system, is able to give answers to the questions asked by users²⁵. You can create artistic content, strings of computer codes, translations in different languages, writing essays and texts in general, reject inappropriate questions and, even, ChatGPT can admit its own error in certain cases. The structure of the software is based on a large language model capable of creating human-like texts based on user input. The answers it provides are very realistic thanks to a machine learning system (known as the Large Language Model (LLM)) based on the processing of the inserted content²⁶. Having clarified the functional aspects of the program, it is useful to analyze the main legal issues

²³F. Casarosa, Cybersecurity Certification of Artificial Intelligence: A missed Opportunity to Coordinate between the Artificial Intelligence Act and the Cybersecurity Act, *Int. Cybersecur. Law Rev.* 3.1 (2022) 115–130.

²⁴J. Mazur, R. Włoch, Embedding Digital Economy: Fictitious Triple Movement in the European Union's Artificial Intelligence Act, *Soc. Leg. Stud.* (2023).

²⁵Van Dis, J. Bollen, R. Van Rooij, W. Zuidema, C. Bockting, ChatGPT: Five Priorities for Research, *Nature* 614.7947 (2023) 223–226.

²⁶*Ibidem*

underlying the decision. What exactly are the criticisms raised by the Italian Privacy Authority? What risks do citizens run when using ChatGPT if the supplier company does not comply with data protection regulations? The Italian Authority has disputed to OpenAI the fact that the data collected from the web by the software does not comply with the regulatory requirements in privacy protection. In particular, the lack of information aimed at ChatGPT users whose data is collected within the platform has been detected. According to the Authority, there would also be no legal basis on which the collection and storage of personal data can be justified for the functioning of the Artificial Intelligence (AI) algorithms underlying the operation of the program. Finally, it was found that the verification of the age limit of users was not respected, which is only allowed to people over 13. In fact, anyone can access the platform, even minors. The problem relating to the processing of collected data, which does not seem to protect users, may, for example, lead to the erroneous association of a particular user's name with defamatory and untruthful content. There is no downstream control and no possibility of correcting the error. Therefore, the Italian Data Protection Authority has opened an investigation the issues raised. It seems that the company has applied "ethical" filters to the software to reduce the risk of providing untruthful news and eliminate the problem of hate speech. However, real answers can be generated, but wrong or without any sense, the algorithm can confuse reality with fantasy and wrong calculations, can fuel misinformation in the medical, political, and legal fields. The risks presented by the Italian Guarantee exist in practice. Further criticism concerns the program's exposure to targeted phishing attacks, in which cybercriminals could manipulate users for the purpose of exchanging personal information to be used for fraudulent purposes. In this sense, cyber security would be affected to the detriment of unaware users. If we consider that after blocking access in Italy, many users have opted for the use of VPNs (a computer tool that simulates access to the internet from another country) to circumvent the obstacle and use the program as a user from other countries. Another important issue is the use of ChatGPT to obtain legal advice. The artificial intelligence system behind the algorithm that provides the answers in the ChatGPT software is not suitable for this purpose and could cause harm to consumers who rely on the program, without verifying the veracity of the information. Finally, as the program has been designed, the answers provided by ChatGPT may be incomplete and incorrect if they refer to information and/or data after the year 2021 (date of the stop of the update of information)²⁷. Subsequently, the provisional limitation order adopted pursuant to Art. 58, para. 2, letter f) of the Privacy Regulation, first provisionally and urgently by the President, was ratified at the plenary meeting of the Office of the Guarantor on 8 April 2023. In the meantime, the company receiving the provisional suspension has contracted with the Italian Authority, by submitting written statements and participating in special meetings. This behavior has led the Guarantor to re-evaluate the compliance with the requirements of the limiting measure provided that OpenAI will implement a series of measures and data protection by the end of April. With the decision of 11 April, the Guarantor therefore suspended the previous measure of 30 March and imposed on the American company a series of actions to adapt to the regulations in the field of the protection of users' privacy. Opposition to this decision may be lodged with the ordinary Judicial Authority within thirty days from the date

²⁷Van Dis, J. Bollen, R. Van Rooij, W. Zuidema, C. Bockting, ChatGPT: Five Priorities for Research, *Nature* 614.7947 (2023) 223–226.

of communication, if the data controller, *Irectius* the company OpenAI, is resident in Italy. Or within the period of sixty days in the case of residence abroad, as it seems to be for the company that in Europe has only a representation, but not even the registered office. Subsequently, the European Data Protection Board (EDPB) set up a task force to promote and facilitate cooperation and exchange information on possible enforcement actions carried out by the various ChatGPT Supervisory Authorities. The task force has developed several considerations and suggestions to guide the regulation of generative AI at European level. It is necessary to consider risks specific to generative AI applications and the fact that they represent a very large category. For this reason, the European regulation on artificial intelligence should take this element in consideration and find valid regulatory tools that also apply to these technologies in the broadest sense (not limited to chatbots and large language models or LLMs). Moreover, generative AI must be regulated throughout the entire product cycle, not only at the application level. It would be useful to consider the variety of actors involved. The initial programming phase is also important because companies developing such software should take a responsible approach to data usage. Therefore, already during this phase, it is necessary to provide mechanisms capable of using the data in an adequate and respectful way of the European rules on the use of personal data. The risk is that if these aspects are not foreseen and regulated software design companies could use the data (more or less consciously) in a way or for purposes not consecrated, making a profit. Following the suspension, the company began to collaborate with the Italian Privacy Authority in order to better manage the situation that has just been described. To this end, several meetings were held until the decision of 12 April, which was made public through a communiqué on the official website of the authority, the Supervisor has decided to propose the creation of a European task force to promote the exchange of information and initiatives related to applications of degenerative AI, such as that of ChatGPT. In addition, the decision provided for a number of indications, recalling the EU legislation on privacy, such as, the necessary compliance with the obligations of transparency and information of the rights of users of the program with the invitation to comply by 30 April. The event ended with the note that the company OpenAI has sent to the Italian Privacy Authority in which it has explained all the measures it intends to take in order to comply with the requests of the provision of the Guarantor announced on 13 April. In particular, the company has undertaken to make available to EU users and, in some extra cases. Finally, the company has announced that it has prepared on its website an information notice addressed to all users to explain how personal data are managed and to comply with the obligations of privacy protection provided by the respective European Regulation. This information will be published on the company's website as soon as the European legislation requiring it (AI Act) comes into force. The company stated that it carried out the following activities: a) expanded the information on data processing reserved for users of the service making it now also accessible in the registration mask before a user register for the service; b) granted to all people living in Europe, including non-users, the right to object to their personal data being processed for the training of algorithms also through a special form that can be filled online and easily accessible. c) has introduced a welcome screen to the reactivation of ChatGPT in Italy, with references to the new privacy policy and the methods of processing personal data for training algorithms. d) has provided for the possibility for data subjects to have the information deemed incorrect deleted, declaring, as it is, technically unable to correct the errors. e) made it clear in the User Policy that while it will continue to process

certain personal data to ensure the proper functioning of the service based on the contract, it will process their personal data for the purposes of algorithm training, unless they exercise their right of objection based on their legitimate interest. f) has already implemented a module for users in recent days that allows all European users to exercise the right of opposition to the processing of their personal data and thus be able to exclude conversations and their history from the training of their algorithms. g) has inserted in the welcome screen reserved for Italian users already registered for the service a button through which, to return to the service, they must declare that they are over the age of eighteen and, in this case, to have parental consent. h) has included in the service registration form the request for the date of birth, providing for a blocking of registration for users under the age of 13 and providing for, in the case of users over the age of 13 but underage who must confirm that they have parental consent to use the service. For this reason, the Italian Data Protection Authority announced in a note published on 28 April that it will consider the cooperative behavior of the company in the investigation. Finally, it is better to wait for the outcome of the proceedings of the Italian Privacy Supervisor to understand what will be the legal and regulatory developments of the case that could have important consequences for other EU Member States as well as the use of generative AI apps

5. Conclusions

As pointed out in this document, the legal consequences and the ethical and technological use of AI-based programs have great importance if we would like to integrate new technological tools safely into modern society. Software like generative AI represent a great opposing unit of development for individuals and action and, at the same time, are a source of important risks to be managed. In the same way, possible risks, such as truthfulness of the data collected, manipulation and distortion of data, technological barriers, and the social and environmental impact of technology, must be considered. There are no secondary ethical aspects related to the use of information and the protection of the privacy of the people involved. Probably, is necessary to integrate data collection with indications of the social, political, and economic context and therefore an interdisciplinary and easily comparable approach. It seems useful, on the one hand, to adapt the regulations in the field of AI, and, on the other hand, to find new ways of cooperation between all the players in the innovative sector, civil society and institutions in order to better protect end-users and detect the risks arising from the misuse of data that such software requires. In this context, the new European Regulation on AI (AIA) is an important regulatory model to be studied in detail. The AI Act is a first worldwide attempt at comprehensive and organic regulation of artificial intelligence, based on the risk management approach. As emerges from the analysis made there are gaps to be filled, such as the need for specific and broader protection forecast in relation to Generative AI applications. The European Union has taken an important step in the direction of protecting and regulating the use of applications based on Artificial Intelligence systems, including aspects of responsibility and risk management. It is useful to see the future development of the discipline, in the knowledge that these rules should be as shared and discussed among all operators in the industry in a collaborative way. In this sense, the comparative approach as well as the sharing of critical issues and risks in the supply chain of AI applications could prove useful and successful. In

conclusion, we must consider the ethical and legal issues that emerged and the risk of confusing the literary texts created by humans with those produced by artificial intelligence (AI) systems, such as ChatGPT. In addition to the risks highlighted, the possibility of misuse of the program, with fraudulent intent or unsuitable for minors, in violation of the rules on the protection of personal data must be considered. In the short term, more than in the past, the problem of legal recognition and the protection of intellectual and literary works elaborated by elaboration of artificial texts will also arise. There is a need to develop a greater awareness of the importance of the protection of personal data by users so that they are able to recognize potential risks and find adequate safeguards.

References

- [1] McCarthy, M. L. Minsky, N. Rochester, C. E. Shannon, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, *AI Mag.* 27.4 (2006).
- [2] N. Purtova, The law of everything. Broad concept of personal data and future of EU data protection law, *Law, Innov. Technol.* 10.1 (2018) 40–81.
- [3] M. Ebers, V. Hoch, F. Rosenkranz, H. Ruschemeier, B. Steinrotter, The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS), *Multidiscip. Sci. J.* 4 (2021) 589–603.
- [4] M. Bussani, L'Unione Europea Al Grande Passo: Verso Una Regolazione Di Mercati E Servizi Digitali, *Quad. Costituzionali* (2021) 224–227.
- [5] G. Resta, B. Carotti, G. Squeo, A. Simoncini, O. Pollicino, M. Libertini, G. Finocchiaro, L. Torchia, La Regolazione Digitale Nell'Unione Europea, *Riv. Trimest. Dirit. Pubblico* 4 (2022) 791.
- [6] I. De Matos Pinto, The Draft AI Act: A Success Story of Strengthening Parliament's Right of Legislative Initiative?, *ERA-Forum* 22.4 (2021) 619–461.
- [7] R. J. Neuwirth, *The EU Artificial Intelligence Act*. Milton: Taylor Francis Group, Law Emerg. Technol. Milton: Taylor & Francis Group (2022).
- [8] D. Svantesson, The European Union 'Artificial Intelligence Act': Potential Implications for Australia, *Altern. Law J.* 47.1 (2022).
- [9] H. Cappelen, J. Dever, *Making AI Intelligible : Philosophical Foundations*, 2021.
- [10] H. Ruschemeier, AI as a Challenge for Legal Regulation – the Scope of Application of the Artificial Intelligence Act Proposal, *ERA-Forum* 23.3 (2023) 361–36.
- [11] P. Hacker, A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act, *Law, Innov. Technol.* 13.2 (2021) 257–301.
- [12] J. Mökander, J. Prathm, D. S. Watson, L. Floridi, The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?, *Minds Mach.* 32.4 (2022) 751–758.
- [13] F. Casarosa, Cybersecurity Certification of Artificial Intelligence: A missed Opportunity to Coordinate between the Artificial Intelligence Act and the Cybersecurity Act, *Int. Cybersecur. Law Rev.* 3.1 (2022) 115–130.
- [14] T. İnce, Salih, European Union Law and Mitigation of Artificial Intelligence-Related Discrimination Risks in the Private Sector: With Special Focus on the Proposed Artificial

- Intelligence Act, *Ann. Fac. Droit D'Istanbul* 71 (2022) 265–307.
- [15] J. Mazur, R. Włoch, *Embedding Digital Economy: Fictitious Triple Movement in the European Union's Artificial Intelligence Act*, *Soc. & Leg. Stud.* (2023).
- [16] Van Dis, J. Bollen, R. Van Rooij, W. Zuidema, C. Bockting, *ChatGPT: Five Priorities for Research*, *Nature* 614.7947 (2023) 223–226.