PRIVACY IN THE AGE OF AI

BY ISHITA VERMA
STUDENT AT UPES, DEHRADUN

INDEX

I. INTRODUCTION

Artificial intelligence (AI) is one of several modern approaches to achieve machine intelligence equal to human intelligence. Other approaches include mimicking the brain, biological cognition, and human-computer interfaces by organizing networks (e.g., the Internet) into a form of collective intelligence. Among these technologies, artificial intelligence has achieved considerable success and is very present in daily life. Artificial intelligence is described as a research field that deals with the creation of intelligent entities and has numerous applications in various fields, such as games, mathematical theorems, and driving.[1]

Artificial intelligence is a branch of computer science. It seeks to understand the nature of intelligence and to develop a new type of intelligent machine that can react in a manner similar to human intelligence. Since the dawn of artificial intelligence, the theory and technology have become more and more sophisticated and the scope is constantly expanding. We can imagine that the technological products produced by artificial intelligence in the future will be the "container" of human intelligence. Artificial intelligence can simulate the information process of human consciousness and thinking. Artificial intelligence is not human intelligence, but it can think like humans and eventually surpass human intelligence. In life, everyone has a personal secret that they do not want others to know and that has nothing to do with the legitimate interests of other people. In law, this secret is called privacy, e.g., personal privacy, diaries, photo albums, life habits, confidentiality of communications, physical defects, and so on. It is a personal right to keep one's secrets from others[2]. This right is called the right to privacy. In the Internet society, however, personal privacy has become a kind of commodity. In the darkness of the Internet, personal privacy is marked and sold. For this reason, the protection of privacy has become urgent, both from a legal and an IT perspective.

II. WHAT IS AI

A system that thinks logically is designed to obey the laws of reasoning. These laws include the law of contradiction, the law of excluded means and the principle of identity. The aim of these systems is to build correct argumentative structures coherently from a correct premise. In other words, they are systems designed to rigorously use logic to solve problems, which presents certain difficulties. One such difficulty is how to transform informal knowledge (e.g. derived from unstructured data) into meaningful logical semantics. Another is how to prioritize information decisions when the amount of information can be overwhelming. This leads to computational time constraints in deciding which information should be considered relevant, particularly in situations of uncertainty.[3]

Artificial intelligence is a form of "intelligent computing"[4] in that it relies on computer programs capable of feeling, thinking, learning, acting and adapting like human beings.[5] It is

[1] Karl Manheim, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 Yale J.L. & Tech. (2019).

[2] Zhizong Chen 2020 IOP Conf. Ser.: Mater. Sci. Eng. 750 012103

[3] Cheng-Kai Liu,Ching-Yen Tu,Hsing-Ru Lin,Ko-Ting Cheng. Asymmetrical transmission windows for daily privacy protection using cholesteric liquid crystals[J]. Optics and Laser Technology,2020,121.

[4] Scientists may call this "computational intelligence," which Al is subset of.

[5] FUTURE of Artificial Intelligence Act, H.R. 4625, 115th Cong. 3 (2017)

"intelligent" because it mimics human cognition.[6] It is "artificial" because it relies on computer processing of information rather than biology. The emerging power of AI stems from the exponential growth of computer processing and storage, and the vast reserves of data that can be mined for meaning. The computing power of machines and advances in robotics are now so impressive that many science-fiction predictions of the past seem to pale in comparison. With quantum computing on the horizon, AI capabilities will improve faster than we can imagine or prepare for.[7]

III. HOW DOES AI WORK

The roots of AI date back to the early 20th century, when pioneers like Alan Turing laid the groundwork for computing machines capable of performing tasks that once seemed destined for the human mind. In recent decades, AI research and development has experienced explosive growth, fuelled by the advent of Big Data, cloud computing and powerful computing resources. The advent of AI has brought with it enormous potential for the promotion and protection of human rights. On the one hand, AI-powered applications improve access to education and healthcare in disadvantaged areas, promoting inclusion and equality.[8] On the other hand, AI's predictive capabilities have the potential to revolutionize criminal justice, reduce miscarriages of justice, and ensure fair trials. However, the downsides of AI development should not be overlooked: Algorithmic biases and discriminatory practices in AI systems pose significant threats to human rights and create systemic inequalities. Moreover, the relentless pursuit of data-driven knowledge has raised serious privacy and data protection concerns. As AI algorithms collect large amounts of personal information, the risk of exploitation and surveillance has increased.[9]

Machine learning is a tool for designing and implementing AI systems and relies heavily on statistical methods to achieve its goals. While an AI system perceives the environment using sensors and executes actions using actuators, machine learning enables the system to learn from experience. Machine learning research contributes to solving important problems in the field of AI, such as how systems can be autonomously improved and what statistical and computational information laws apply to learning systems. A machine learning system is created through a training process to produce a model that predicts future outcomes based on new inputs. Typically, machine learning models are created through supervised, unsupervised, semi-supervised, or reinforcement learning. Recent trends in machine learning include increasingly complex models that work with larger and larger amounts of data.[10]

[6] Algorithms Based On Brains Make For Better Networks, NEUROSCIENCE NEWS (July 17, 2015), https://neurosciencenews.com/neuroscience-network-algorithms-2263.

[7] Wei Kong,Jian Shen,Pandi Vijayakumar,Youngju Cho,Victor Chang. A practical group blind signature scheme for privacy protection in smart grid[J]. Journal of Parallel and Distributed Computing,2020,136.

[8] Begum, S. (2023). AI Odyssey: Unraveling the Past, Mastering the Present, and Charting the Future of Artificial Intelligence.

[9] Rajan Rayhan, *AI and Human Rights: Balancing Privacy and Innovation in the Digital Age*, Research Gate (2023).

[10] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends perspectives and prospects", *Science*, vol. 349, no. 6245, pp. 255-260, 2015

IV. CONCERNS ABOUT AI

While the use of AI on par with human intelligence has benefits, such as promoting rapid technological development, it also raises a number of public concerns, ranging from economic instability to apocalyptic consequences. There is growing public concern about privacy violations by AI-enabled devices, especially after the advent of personal assistants such as Google Home and Amazon Alexa. Stories and articles about these devices spying on people and recording speech habits do not promote public acceptance of AI[11].

A consensus showed how deep neural networks can be trained to classify a person's sexual orientation based on facial features with 91% accuracy. This technology has immediate privacy implications as it provides a mechanism for revealing a person's sexual orientation that they would otherwise not want to disclose. More seriously, in oppressive regimes, sexual orientation becomes a matter of life and death, and AI developments pose a much greater risk to the oppressed. Moreover, the data used for training and the features used in practice have direct privacy implications. [12]

Artificial intelligence (AI) is becoming more ubiquitous in our lives as it permeates the digital services we use and the physical devices we own. The most widely used digital services such as search (Google, Bing), music (Spotify, YouTube Music), entertainment (Netflix, YouTube), and social media (Facebook, Instagram, Twitter) already rely on AI or machine learning (ML) to provide users with personalized content and enhanced features such as relevant search results, content that users like, and people they know. AI also enhances various physical devices we own (or could own), such as smart speakers like the Google Hub and Amazon Echo, which rely on natural language processing to recognize and understand speech and execute commands, e.g., to control lighting, change the temperature, or add groceries to the shopping list. Using AI to deliver highly personalized experiences benefits both users and providers: users gain positive engagement with these platforms and providers gain engaged users who spend more time using their services.[13]

The ability of artificial intelligence to surpass human intelligence is the subject of lively debate. The Turing Test is an experiment in which a human interviewer, in a blind conversation, is unable to distinguish between human-generated and computer-generated natural language responses. Futurologist Ray Kurzweil has predicted that the Turing test will be passed in 2029. Until then, we will remain in the era of Narrow Artificial Intelligence (NAAI) or Weak Al, in which specialized computer programs outperform humans in certain tasks such as games of skill and text analysis. ANI also includes cognitive computing, in which machines assist humans in tasks such as the reading of X-rays by radiologists, the processing of transactions by stockbrokers and the drafting of contracts by lawyers.[14]

[11] G. Fowler, “Perspective—Alexa has been eavesdropping on you this whole time”, May 2019, https: //www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/.

[12] J Curzon, *Privacy and Artificial Intelligence*, 2 IEEE Transactions on Artificial Intelligence (2021).

[13] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 308–318.

[14] Rajan Rayhan, *AI and Human Rights: Balancing Privacy and Innovation in the Digital Age*, Research Gate (2023).

V. AI-RELATED PRIVACY ISSUES

AI technology increases the ability to collect, analyze and aggregate incredibly large amounts of data from multiple sources to an unprecedented level. What's more, this type of technology is now widely accessible to all types of people and organizations worldwide. Although information technologies have already had an impact on privacy, this new capability greatly increases the potential for privacy breaches that were not previously considered.

A common method of assessing privacy breaches is to carry out a Privacy Impact Assessment (PIA). Performing an effective privacy impact assessment is itself an evolving area of research, in which current methodologies and frameworks can be borrowed and applied to AI. Guidelines such as those in suggest starting a PIA as early as possible and include detailed methodologies. CNIL guidelines suggest a compliance-based approach to assessing privacy protection factors, taking into account the fundamental principles of data subject rights to identify and mitigate risks.[15] The phases of a data protection impact assessment include preliminary analysis, project analysis, data protection analysis and report preparation. Here, we focus on the privacy analysis phase and how it might be applied to AI as a whole.

i. AI challenges and threats to human rights

As AI becomes increasingly integrated into our lives, concerns about possible human rights violations have grown. The use of biased historical data can lead to discrimination and thus to unfair treatment and inequitable decisions - from recruitment practices to the granting of credit. In addition, AI's insatiable appetite for data has raised serious data protection concerns. As AI systems collect, process and analyze vast amounts of personal data, individuals are increasingly vulnerable to data mining and surveillance. The commercialization of personal data in turn threatens the right to privacy and autonomy.

ii. The Internet of Things

The power of artificial intelligence lies in machines' access to data. This is essentially what AI does: it crushes data. So, the more information there is on a subject, or the larger the accessible data set, the better Al can respond to a request or perform an operation. The Internet of Things ("IoT") is an ecosystem of electronic sensors present in our bodies, homes, offices, vehicles and public spaces.[16] By "objects", we mean any physical or artificial object that is assigned an Internet address and transmits data over a network without interaction between humans or between humans and computers. If Al is like the human brain, the IoT is like the human body, collecting sensory data (sound, sight and touch). IoT devices collect raw data on humans performing physical and other actions. These devices have facilitated the collection, storage and analysis of vast quantities of information. [17]

iii. AI intrusion into privacy.

Even if an individual has never provided complete personal information to a network platform or institution, AI still has the potential to fully integrate the privacy of any Internet

[15] J. A. Perez, F. Deligianni, D. Ravi and G.-Z. Yang, "Artificial intelligence and robotics", 2018.

[16] Jonathan Shaw, Artificial Intelligence and Ethics, HARV.MAG. (Jan.-Feb. 2019), https://www.harvardmagazine.com/2019/01/artificial-intelligence-limitations.

[17] Sadia Din et. al, A Cluster-Based Data Fusion Technique to Analyze Big Data in Wireless Multi-Sensor Systems, IEEE ACCESS (Feb. 2, 2017), https://ieeexplore.ieee.org/document/7873266

user with corporate data through non-standard integration data mining technology and personal network behavioural profiling.[18] It mainly comprises four steps: information discovery, information integration, attribute analysis and user portrait. Privacy data integrated by AI can be used for various promotions and sold directly to offenders for illegal purposes.

iv. Data collection and use by AI technologies

One of the most important implications of AI technology is the way it collects and uses data. AI systems are designed to learn and improve by analyzing large quantities of data. As a result, the amount of personal data collected by AI systems is constantly increasing, raising questions about privacy and data protection. We only need to take a look at various creative AI tools such as ChatGPT, Stable Diffusion or others in development to see how our data (articles, images, videos, etc.) is used, often without our consent.

Above all, the use of personal data by AI systems is not always transparent. The algorithms used in AI systems can be complex, and it can be difficult for individuals to understand how their data is used to make decisions that affect them. Lack of transparency can lead to distrust of AI systems and a feeling of unease. To address these concerns, it’s important that organizations and companies using AI technology take precautions to protect individual privacy. These include implementing robust data security protocols, ensuring that data is only used for its intended purpose, and developing AI systems that adhere to ethical principles.

Of course, transparency in the use of personal data by AI systems is crucial. Individuals must be able to understand how their data is used, and control how it is used. This includes the possibility of refusing data collection and requesting its deletion. In this way, we can shape a future in which AI technologies are used for the benefit of society, while protecting individual privacy and data.

v. The use of AI in surveillance

One of the most controversial uses of AI technology is surveillance. AI-powered surveillance systems have the potential to revolutionize law enforcement and security, but they also pose significant risks to privacy and individual freedoms.

AI-powered surveillance systems use algorithms to analyze large amounts of data from multiple sources, such as cameras, social media and other online sources. This enables law enforcement and security agencies to track individuals and predict criminal activity before it occurs. While the use of surveillance systems powered by artificial intelligence may seem a valuable tool in the fight against crime and terrorism, it also raises concerns about respect for privacy and civil liberties. Critics argue that these systems can be used to monitor and control individuals, with a potential loss of civil liberties and rights.

To complicate matters further, the use of surveillance systems powered by artificial intelligence is not always transparent. It can be difficult for individuals to know when they are being monitored or for what purpose. This lack of transparency can undermine trust in

[18] Ian Bogost, Welcome to the Age of Privacy Nihilism, ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198.

police and security services, and create a sense of unease among the population. To address these concerns, the use of surveillance systems based on artificial intelligence needs to be strictly regulated and controlled. This implies the development of clear policies and procedures for the use of these systems, as well as the establishment of independent control and review mechanisms.

Law enforcement and security agencies should be transparent about when and how these systems are used, and individuals should have access to information about how their data is collected and used. The integration of surveillance systems powered by artificial intelligence has undoubtedly brought significant benefits to law enforcement and security agencies. However, it is essential to recognize the potential risks of these systems to our fundamental rights and freedoms. Lack of transparency and the risk of discrimination are just some of the concerns that regulators must address to guarantee the protection of privacy and individual freedoms. Implementing robust regulations and control mechanisms is an essential step in creating a future where AI technologies are used for the benefit of society without compromising individual rights and freedoms. It is important to establish clear policies and procedures that regulate the use of AI-based surveillance systems and guarantee transparency in their implementation. In addition, independent monitoring and review mechanisms should be put in place to ensure accountability.

VI. PRIVACY AND DATA PROTECTION IN THE AGE OF ARTIFICIAL INTELLIGENCE

The interaction between AI and privacy is a complex and multifaceted issue. In the age of data-driven decision-making, the implications of AI for individual and collective privacy are profound, and understanding them is paramount for policymakers and the general public alike. In the age of AI, privacy has become an increasingly complex issue. With so much data being collected and analyzed by companies and governments, individuals' personal information is more at risk than ever.

These issues include intrusive surveillance, which can erode an individual’s autonomy and exacerbate power imbalances, and unauthorized data collection, which can compromise sensitive personal information and leave individuals vulnerable to cyber-attacks. These problems are often exacerbated by the power of BigTech companies, which hold vast quantities of data and exert considerable influence over how it is collected, analyzed and used.

The exponential growth of data-driven technologies, coupled with the ability of artificial intelligence to process vast quantities of information, poses major challenges for privacy and data protection. As AI systems collect data from different sources, the risk of privacy breaches and unauthorized access increases. Strategies for reconciling innovation and data protection in the AI era include robust data anonymization techniques and ensuring that AI algorithms prioritize data minimization. In addition, applying data protection principles at the design stage can foster the development of AI systems that inherently respect people’s right to privacy.

Even if we manage to strictly protect all data and limit AI to its intended use, there is no guarantee that this use will not harm consumers. Predictive algorithms often assume that there is a hidden truth to be learned, such as consumers' gender, income, place of residence, sexual orientation, political preferences or willingness to pay. But sometimes, the "truth" to be learned evolves and is subject to external influences. In this sense, the algorithm may intend to find the truth, but it ends up defining it itself. This can be damaging, as algorithm designers use them to serve their own interests, which may conflict with those of consumers, such as the pursuit of profit, the quest for political power or the promotion of cultural change. The danger of deceptive algorithms has already been highlighted in the controversy over how Russian-sponsored contributions were disseminated on social media during the 2016 US presidential election[19]. At congressional hearings on October 31 and November 1, 2017, lawmakers expressed concern that Facebook, Twitter and Google's business model, which relies on advertising revenue from a large user base, could hamper their willingness to detect or limit misinformation from problematic users[20].

VII. PRIVACY PROTECTION LAWS AROUND THE WORLD T

i. Privacy protection in the USA

The United States is home to some of the world's largest and most advanced technology and data companies. Experts attribute their dominance of the international market to the absence of comprehensive federal regulations to protect personal data and privacy. Instead, the USA relies on a "sectoral approach" consisting of a patchwork of sector-specific federal laws, often enforced by different agencies and setting different standards.

In contrast, the European Union (EU) and many other developed countries adopt a comprehensive approach with a single law that uniformly regulates data collection, use and disclosure across all sectors. For example, the EU's General Data Protection Regulation (GDPR) is a general regulation that applies across all sectors and member states to all entities that are "established" in the EU, provide goods or services in the EU or serve people in the EU . [21]

Many US companies initially preferred a sectoral approach, in order to tailor the rules to their specific needs. While this model has some validity, it also facilitates regulatory capture, industry pressures and privacy abuses that often escape the regulatory net. The sectoral approach has created a patchwork of federal and state laws that "overlap, intersect and contradict each other".

ii. European privacy legislation

Unlike the US regulatory regime, the European Union's General Data Protection Regulation (GDPR), which came into force on May 25, 2018, has had serious repercussions. Violators face administrative fines of up to twenty million euros or four percent of a company's

[19] Roberrt S. Mueller, III, Report on the Investigation Into Russian Interference in the 2016 Presidential Election (March 2019), https://www.justice.gov/storage/report.pdf. A searchable version is available at Read the Muller Report, N.Y. TIMES (April 18, 2019), https://www.nytimes.com/interactive/2019/04/18/us/politics/mueller-report-document.html.

[20] https:// www .nytimes .com/ 2017/ 09/ 07/ us/ politics/ russia- facebook- twitter- election .html, accessed on October 19, 2017. http:// money.cnn .com/ 2017/ 09/ 28/ media/ blacktivist- russia - facebook- twitter/ index .html, accessed on October 19, 2017.

[21] Mark Rotenberg, On International Privacy: A Path Forward for US and Europe, HARV. INT'L REV. (June 15, 2014), http://hir.harvard.edu/article/?a=5815.

worldwide annual turnover, whichever is higher.311 As a result, tech giants such as Google have been forced to modify their behaviour in response to the GDPR's sanctions.[22]

The difference between US and EU approaches to privacy can be explained in part by Europe's experience during the Second World War. After the war and the creation of the United Nations, many countries recognized that fundamental human rights needed to be protected to support democratic institutions. In 1948, Article 12 of the Universal Declaration of Human Rights (UDHR) established principles that included privacy as a fundamental human right. Article 19 provides broad protection for privacy rights. Article 19 provides broad protection for freedom of expression. The EU drafted the GDPR as a regulation directly binding on all member states. The aim was to create a coherent data protection framework with strict enforcement and enhanced rights for individuals.[23] By giving individuals greater control over their data, the GDPR strengthens trust in the digital economy and online environment. Control, transparency and accountability are recurring themes of the GDPR.

iii. <u>The Indian perspective</u>

At present, there is no specific law governing AI in India. The Ministry of Electronics and Information Technology (MEITY) is the executive agency for AI-related policies and has formed committees to create a policy framework for AI. The Niti Ayog has developed a set of seven principles for responsible AI, which include safety and reliability, fairness, inclusion and non-discrimination, privacy and security, transparency, accountability and the protection and enhancement of positive human values.[24] The Supreme Court and the High Courts have a constitutional mandate to uphold fundamental rights, including the right to privacy. The principal privacy legislation in India until now has been the Information Technology Act and its implementing regulations.

The Digital Personal Data Generation Bill 2023, presented in its current form to the Lok Sabha, has forced the technology industry, particularly those working with AI and ML, to rethink the way they operate and process data. As legal experts have pointed out, no company can afford to be lax in its handling of data any longer. That's why AI companies and developers have a lot of work to do. The bill has influenced the logic of building and training AI models to create chatbots or other services. From where and how data is obtained, to what happens to data after it has been used to train AI models, AI developers and development studios will now need to obtain permissions for many things and ensure that they have legally implemented all the necessary compliance rules.

The Digital Personal Data Protection Act (DPDP Act) 2023 is now imminent, meaning India has a shiny new data protection law. The Act provides a protective barrier by defining compliance expectations for data fiduciaries (those who collect and process data digitally) versus data principals (the people who hold the data). The law has come as a great relief at a time when the use of artificial intelligence-based applications trained on large amounts of

[22] Regulation (EU) 2016/679 of European Parliament and of Council of 27 April 2016 on protection of the natural person(s) with regard to processing of the personal data and on free movement of data.
[23] Mark Rotenberg, On International Privacy: A Path Forward for US and Europe, HARV. INT'L REV. (June 15, 2014), http://hir.harvard.edu/article/?a=5815.
[24] Niti Aayog, *Adopting the Framework: A Use Case Approach on Facial Recognition Technology*, NITI AAYOG (Nov. 1, 2022), https://www.niti.gov.in/.

personal data is becoming increasingly popular. Despite the relief that personal data must be collected and processed in accordance with the law, India’s Digital Personal Data Protection Act 2023 has several shortcomings that it fails to address.

Firstly, there are no provisions regulating the purposes for which data may be collected and used, provided that the purpose is lawful. The law, as passed, allows administrators to collect data for any lawful purpose, provided that it is lawful. This means that algorithms that track personal preferences and advertisements that exploit a user's personal data and online behaviour (dark patterns) can be used freely, except in the case of children. [25]

Secondly, the success of the law depends on the country’s citizens being aware of their rights and being able to enforce them using the complaints mechanism provided for in the Data Protection Act. The law does not oblige the DPA or any other authority to inform citizens of their rights under GDPR or to check compliance with administrators or data controllers. Nor is there any obligation to proactively mitigate damages. In light of these facts, the GDPR law, while well-intentioned, lacks the force of enforcement. [26]

Many of these ambiguities should be resolved when the provisions of the DPDP Act are challenged in the courts. In the meantime, it is to be hoped that MEITY will proactively amend the law or issue regulations to clarify the issue.

iv. EU AI Act

The proposed regulation establishing harmonized standards for artificial intelligence, better known as the EU AI Act, will be finalized by the end of the year. Pending final EU procedures, the act will probably be adopted in early 2024, before the European Parliament elections in June 2024. Adoption will be followed by a transition period of at least 18 months before the regulation comes fully into force.

The AI Act is a legal framework regulating the sale and use of AI in the EU. Its official aim is to ensure the smooth operation of the EU single market by setting uniform standards for AI systems in all EU member states. In practice, it is the first comprehensive piece of legislation to address AI-related risks through a set of obligations and requirements aimed at safeguarding the health, safety and fundamental rights of citizens in the EU and beyond, and is expected to have a significant impact on AI governance worldwide.

The AI law applies to AI systems “placed on the market, ordered or used” in the EU. This means that, in addition to EU developers and designers, it also applies to global suppliers who sell or make their system or its results available to EU users. [27]

[25] Nivedita Krishna, *The Digital Personal Data Protection Act, 2023: Some relief but many questions*, TIMES OF INDIA (Oct. 29, 2023), https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/the-digital-personal-data-protection-act-2023-some-relief-but-many-questions/.

[26] Nivedita Krishna, *The Digital Personal Data Protection Act, 2023: Some relief but many questions*, TIMES OF INDIA (Oct. 29, 2023), https://timesofindia.indiatimes.com/blogs/niveditas-musings-on-tech-policy/the-digital-personal-data-protection-act-2023-some-relief-but-many-questions/.

[27] Mia Hoffmann, *The EU AI Act: A Primer*, CSET (Sept. 26, 2023), https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/.

There are three exceptions:[28]

- AI systems developed or used exclusively for military purposes and potentially on a larger scale for defense and national security purposes, pending negotiations,
- AI systems developed and used for scientific research purposes; and
- free AI systems and components (a term that is not yet clearly defined), with the exception of the basic models discussed below.

AI systems that fall into the category of unacceptable risks are banned outright. According to the consensus between the three proposals, systems with unacceptable risks include those with significant potential for manipulation, either through subliminal messages and stimuli, or by exploiting vulnerabilities such as socio-economic status, disability or age. Also banned are artificial intelligence systems for social evaluation, a term used to describe the assessment and treatment of people on the basis of their social behaviour. The European Parliament also wants to ban real-time remote biometric identification in public places, such as live facial recognition systems, as well as other uses of biometric and law enforcement systems.[29]

VIII. CONCLUSION

Privacy issues related to AI are a fundamental question that must be taken seriously. As the capabilities of computer systems increase, so do those of AI systems. Violations of privacy in any form are also an affront to human rights and democratic values. The difficulty in assessing the risk of privacy violation in the context of AI lies in the adaptive and evolutionary nature of the field, since AI is the result of the fusion of different domains with the aim of creating something superior to its parts.

To protect privacy in AI systems, each system component must be considered separately in relation to privacy contexts. In the current state of AI, privacy risks dominate in knowledge representations, NLP, automatic reasoning and the creation, operation and use of machine learning models. Addressing privacy risks in AI systems is not an easy task, and is an undertaking that will continue to evolve as AI develops. Therefore, future work in the field of privacy in AI will benefit from a continuous reassessment of how component technologies contribute to privacy risk and how they interact with each other in an AI system.[30]

Consumer privacy and data security pose pressing issues, many of which are likely to be reshaped by AI and other data technologies. Big questions arise: should we continue to let the market develop on the basis of existing laws, or should we be more aggressive in government regulation? How do companies choose technology and data policy when consumers demand both convenience and privacy? How do we balance the innovation enabled by AI with the additional risk this same technology poses to privacy and data security? If policymakers must act, will we let local governments proceed by trial and error, or insist on federal legislation at

[28] Shana Lynch, *Analyzing the European Union AI Act: What Works, What Needs Improvement*, Stanford University HAI (July 21, 2023), https://hai.stanford.edu/news/analyzing-european-union-ai-act-what-works-what-needs-improvement.

[29] Mia Hoffmann, *The EU AI Act: A Primer*, CSET (Sept. 26, 2023), https://cset.georgetown.edu/article/the-eu-ai-act-a-primer/.

[30] H. Wang, S. Gong, X. Zhu and T. Xiang, "Human-in-the-loop person re-identification", Proc. Eur. Conf. Comput. Vis., pp. 405-422, 2016.

the national level? Will we wait for new laws to fill ongoing gaps, or rely on the judiciary to clarify existing laws on a case-by-case basis? These questions deserve the attention of researchers from many different disciplines, including economics, computer science, information science, statistics, marketing and law.

Some scientists, philosophers and futurologists have sounded the alarm about the existential threat posed to humanity by Al and autonomous robots. We don’t go that far. But it seems inevitable that Al will have far-reaching implications for constitutional rights and democratic institutions. We may not have to stop Al, but we will certainly have to pay attention.

At the dawn of the 21st century, the proliferation of artificial intelligence (AI) technologies has ushered in a new era of unprecedented ease, innovation and efficiency. From virtual personal assistants to autonomous cars, from recommendation algorithms to medical diagnostics, AI has become an integral part of our daily lives. But with these remarkable advances comes an urgent concern that has caught the attention of individuals, organizations and governments around the world: maintaining privacy in the AI age.