Ensuring that AI technologies are regulated and consumer protections are secured.

Tables of contents

Overview

The introduction of AI (Artificial Intelligence) has brought new, and sometimes unexpected, advantages and disadvantages to the world. It has presented many desperate individuals with innovative resolutions and increased life quality, though it also infringed on consumer protection, such as misleading information and breaches in privacy, putting many people in trouble.

AI technologies, unlike general technologies, are capable of learning and adaptation. While general technologies mainly function on pre-coded algorithms, AI technologies show better flexibility through collecting and analysing new data; ultimately adapting itself to the user's niche (1). Due to its smart algorithm, affordable hardware, and increased accessibility to users, AI is gaining more popularity among its consumers (2) and is taking up a large part in our daily lives. For example, AI assistants such as Siri and Alexa, personalised recommendations in social media, biometric profiling, and location detection in navigation are all AI-enabled technologies (3). As much as AI has infinite potential in its ability and is commonly used nowadays, the disadvantages cannot be further ignored, as the widespread use of AI magnifies the effects on people.

One of the many infringements on consumer protection is the violation of privacy rights. AI gathers unimaginable amounts of data to further enhance its algorithm through data training. However, during the process, it gathers private data of individuals with the possibility of leaking it in public, breaching individual privacy rights. This resulted in internet users demanding their privacy rights to ensure data collection under their consent. Yet, even with consent, data may be misused beyond what the user has given consent to, posing a challenge in AI technology regulations in data collection. Furthermore, some AI models gather data beyond the internet, as some are used to analyse surveillance data, and can access surveillance devices such as security cameras (4). For instance, China has AI-enabled surveillance cameras installed in many public spaces. Because these AI-enabled technologies are used for national security and sovereignty, these cameras have biometric profiling and facial recognition systems integrated, and the vast amount of highly sensitive information these cameras have access to increases the potential damage that civilians will experience. Highlighting that China shares these technologies with other regions such as Southeast Asia, Central Asia, Africa, and the Middle East, Member States need to set strict regulations regarding individual privacy regarding surveillance cameras (9).

Another example is consumer fraud, referring to actions such as financing done unjustly through deceptive methods, commonly known as a scam. Nowadays, more than 50% of fraud in 2025 has incorporated AI for purposes of generating fake identities and realistic photos, widely known as deepfake media, to buy trust from target consumers and take over accounts or money. To combat this, banks also incorporate AI to detect fraud, but face more obstacles relative to the criminals. For instance, while criminals' only objective is to abuse technologies to their benefit, banks have to consider possible ethical challenges the detection AI can cause and ensure that the AI used is legally appropriate, limiting its ability compared to the criminals (5). To combat these manipulative AI misuses, the European Union (EU) proposed the AI Act in 2021, which will be further explained in detail in the next section, to enhance European citizens' privacy rights and security regarding AI usage. The Act classifies AI-enabled technologies in four categories: unacceptable risk, high risk, limited risk, and minimal risk. Technologies that are classified as unacceptable risk if they are used for manipulative or deceptive purposes, and they are banned. Though this AI Act only legally binds EU nations, some nations, such as Brazil, South Korea, and some states of the United States of America, have adopted similar legislation. To minimise further harm caused by deceptive AI use, it is highly recommended that Member States have a common agreement on a regulation like the EU AI Act (10).

The third example of violation in consumer protection is the algorithmic bias and possible discrimination towards users. Many businesses have AI implemented in Human Resources (HR) systems — where HR refers to a business department that manages employees through various tasks, such as organising employee hiring processes (6) — which is becoming a trend among businesses. Among those with AI implementation, 64% of AI use was for talent acquisition — a process of deliberately selecting elite job applicants who can contribute to the business's long term goal instead of recruiting for an immediate job filling (7). Part of the reason for the implementation of AI is due to its high efficiency in decision-making through accurate analysis and prediction, and the aim for bias mitigation during the process. However, counterparties claim that AI, in fact, magnifies bias due to the input it uses for data training. Research identified that because the training data used to set criteria for "an ideal employee for the company" was based on past human bias, the established criteria were also impartial. Additionally, through further analysis of minor implications about the applicant's personal information, such as their gender or race, AI are now able to identify and rank applicants based on its impartial criteria — instead of focusing more on the individual's ability (7). Businesses' initial intention of practising equality through AI is now conversely emphasised by AI, risking consumer protection from discrimination and bias. Although job applicants and consumers are different in a sense of literal definition, in a broader sense, AI systems that are used in the decision-making process treat job applicants as their consumers. Likewise, the system should also have similar core values as consumer protections, such as anti-discrimination and transparency.

However, setting overly strict regulations on these AI technologies may also result in negative impacts on a larger scale. Over-regulations, first of all, will impact the world's AI development rate by setting stricter criteria for safety assessment or limiting the AI's ability, regardless of whether the use of it is beneficial or not. This hence implies that strict regulation of AI may hamper the growth of life-changing AI technologies — such as medical inventions or AI-enabled cybersecurity programs — jeopardising not only those who need immediate medical care, but almost all internet users whose cybersecurity is no longer guaranteed from AI abuse (8). Furthermore, strict regulations may limit engineers and scientists in experimenting with AI's capabilities, restraining them from discovering new uses of AI that contribute to further innovation of technologies (11).

Second, over-regulations can also create unequal opportunities among large businesses and start-up companies due to the limitations as novice companies. When stricter regulations apply to all scales of companies, small companies may lack resources and money to comply with the newly introduced regulations, taking away growth opportunities from start-ups with large potential. For instance, start-ups can attain growth opportunities largely through partnerships with larger businesses or investments. However, after the introduction of the General Data Protection Regulation (GDPR) in 2018, the investment rate in small companies has decreased by 36% due to concerns that the start-ups would not be able to manage new compliance rules (11) (12). Hence, considering how start-ups play an important role in the technology industry, having a regulation that does not impose a huge burden on small start-ups is also important.

Lastly, over-regulations may also impact the economy on an international scale. For instance, China, by collaborating with its firms, is currently using and exporting AI-enabled surveillance cameras with biometric profiling and facial recognition integrated in them. The surveillance cameras are exported to various aforementioned regions for global smart-city projects to enhance public safety and efficiency (9). If over-regulations limit the use of these surveillance cameras, national security may be undermined; companies that manufacture these surveillance cameras and the nations that export them will experience a downfall in their economy. This example is not merely limited to this case of China, but also shows that other international trade regarding AI-enabled technologies is also threatened by limits in AI use. Hence, it is strongly encouraged that the delegates be cautious and draft their resolutions in a way that does not largely impact nations' economies.

In summation, in spite of significant movements made on large scales — such as the AI Act of the EU and the GDPR European law — AI technologies are still posing significant threats without boundaries. However, there are still beneficial sides of these technologies, and

over-regulations may result in more harm by overriding those benefits, such as to the national economy and to the enhancement of technologies. Delegates should therefore have a deep understanding of country stances, especially in terms of how each country is related to AI, and have a fair prediction of possible outcomes per regulation to prevent overcontrol on AI.

Definitions of important terms

Artificial Intelligence (AI)

Artificial Intelligence (AI) is a system capable of learning and adapting skills that were previously thought to be limited only to humans. This made AI technologies exceptionally flexible in their ability to accomplish tasks with variables — such as recognising patterns and problem solving — because they do not necessarily require a pre-coded algorithm like traditional technologies (13). Although there are many cases where AI breaches consumer protection through misuse, its trait as a whole can also directly cause harm. For example, when AI collects data for learning, it may collect biased or sensitive sources. The biased sources may affect AI's decision-making process during talent acquisitions — limiting opportunities to marginalised groups regardless of their competence (7) — while the sensitive sources may leak to the public, breaching civilians' privacy (4).

Consumer protection

Consumer protection is a set of laws and regulations that protect consumers' safety through education, mobilisation, and representation. It ensures that consumers can make fully-informed decisions, successfully revise the decisions, and receive the promised quality products and services. Meanwhile, businesses refrain from deceptive activities that harm consumers. Although it is generally understood that consumers refer to those who buy goods and services, delegates should be aware that there is no universally agreed definition of consumer and its definition may sometimes vary depending on the context or who defines it (14). For example, the way consumers and job applicants were previously linked together shows a broader definition of consumer, which included job applicants. Consumer protection is especially important because it applies to any individual who engages in any type of economic activity, whether it happens online or offline. Therefore, it is not an exaggeration that this is one of the most urgent issues to solve, as these threats from AI will come to every individual.

AI ethics

AI ethics is a set of conduct regarding AI, focusing on human values. Similar to the definition of consumer, there are no commonly accepted principles of AI ethics and organisations such as governments or companies each set their own principles. However, there are still commonly occurring principles such as human dignity — prioritising humans to ensure AI does not replace or compromise human well-being — and upholding data privacy — ensuring AI adheres to strict data privacy rules to prevent data breaching or unapproved access (15). For example, the United Nations Educational, Scientific and Cultural Organisation (UNESCO) has established the first global principles on AI ethics, officially called the Recommendations on the Ethics of Artificial

Intelligence, applicable to all 194 Member States. It consists of four core values and ten core principles, including human dignity and safety and security (16). Moreover, the Association of Southeast Asian Nations (ASEAN) also adopted their own set of core principles on AI ethics. Applicable to all ASEAN regions, this also encompasses human centricity, security, and safety (17). It is therefore crucial for delegates to have a general agreement on these ethical standards to minimise the gaps between varying perspectives.

Black-box AI

Black-box AI is an AI system that lacks transparency in the process of its decisions. While the inputs and outputs are clear, the process that results in the output is hidden from consumers, and sometimes even from the engineers. The lack of transparency in these AI systems not only reduces the credibility of the AI but may also lead to the reflection of the "Clever Hans effect" on significant matters. This effect reflects events where one yields the correct result but with incorrect reasoning. When this effect is applied to vital AI technologies such as healthcare, it can result in serious issues. For example, AI models trained to diagnose COVID-19 using lung x-rays were successful during their training, but showed poor performance in the real world. This was because one of the factors the models considered during their diagnostic process was the X-ray annotations, which were intended to highlight the features that suggested COVID-19. If these models were used in real-life situations, they would most likely have diagnosed all patients as unaffected and caused greater damage to a larger population. What makes it especially demanding to simply set rules to make AI transparent as a resolution is that some machine learning models go through complicated deep learning processes, even challenging the creators to comprehend the process. Hence, simply setting rules to make AI transparent is, on an aspect, unfeasible and delegates are highly encouraged to consider these complications (18).

Human In The Loop (HITL)

Human In The Loop in AI is a system where humans intervene in AI procedures to ensure accuracy, safety, transparency, and ethical decision-making. As mentioned before, mass data collection raises multiple issues, and even the most complex learning process models have their own flaws due to it. In terms of accuracy and safety, HITL mitigates these issues by utilising human intervention to filter biased inputs and rectify misleading outputs, guiding AI towards its improvement over time. In ethical decision-making, human intervention ensures that the decisions made by AI models are ethical and appropriate for the social norm. Although AI has great potential and the capability for a wide range of complex analyses, human perspectives are still sometimes needed, especially when it comes to ethical dilemmas. Lastly, HITL can increase transparency by mitigating the effects of black-box AIs. Through monitoring and controlling the developmental processes and detecting risks, previously opaque AI models can now be inspected and understood, which raises transparency. As shown, HITL needs to be present in most AI

models as they are incomplete in their ability to work independently while guaranteeing safety. Nevertheless, relying on human intervention for an extended period of time also brings a negative effect, as ironically, their functionality can fall short in some aspects. For instance, in cases where the AI systems become more complex, and their data set grows larger, the sheer amount of labour hours and the cost of experts may be unbearable in due time. In addition, while HITL is expected to mitigate bias in AI models, humans themselves may have bias or differing perspectives, leading to HITL incorporating error or inconsistency in its job. Lastly, humans also have the same risk of sensitive data exploitation as AI. Though it may not be intentional, as long as they work with internal data, it is possible to leak or misuse data at some point (19).

Timeline of key events

May 2018: The General Data Protection Regulation (GDPR) comes into effect
The GDPR is a data privacy and security law, which is an important factor when discussing AI technology regulation. It is one of the harshest laws, as it imposes heavy fines on those who violate the law, holding them accountable for up to tens of millions of euros. Though drafted and passed by the EU, the law also applies to any organisations that target EU citizens to collect data, also subjecting organisations outside of the EU to grand fines. Its data protection principles set a guideline to anyone who attempts to process data, which minimises the possibility of personal data being misused or exploited. The principles include standards such as: using data only for the purpose disclosed to the consumers, storing data only as long as necessary for the stated purpose, and, most fundamentally, all data processing should be legal and transparent (20).

May 2019: The Organisation for Economic Co-operation and Development (OECD) adopted "OECD Principles on AI"
The OECD Principles on AI are a set of five value-based principles — which promote AI use in an innovative and trustworthy way while valuing human dignity and democratic factors — and five recommendations for policymakers for effective AI policies (21). As it is the first intergovernmental standard on AI, it is referenced and has become the foundation for many countries' AI policies and frameworks. In 2024, the Principles on AI were revised once again to follow the fast innovation of new AI technologies. The revision tackles multiple growing issues regarding AI. For example, it addresses safety concerns that enable robust mechanisms to rectify erroneous behaviours of AI, reflects the significance of addressing the spread of inaccurate information, and promotes transparency through clarification of information (22).

June 2020: Launch of Global Partnership on Artificial Intelligence (GPAI)
The GPAI is a global initiative that advocates for responsible growth and use of AI, focusing on human rights, inclusion, diversity, innovation, and economic growth. The initiative, therefore, aims to close the gap between theory and practice on AI through support for pioneering research and applied activities on AI-related priorities. Consisting of 44 participant countries, the GPAI is also closely partnered with the OECD and uses the OECD Principles on AI as a foundation to set the trajectory of its work (23)(24). This initiative is a good example of what delegates should focus on, as it not only centres around safe use and development of AI, but also around economic growth and inclusivity. This reflects how the GPAI is maintaining awareness of overregulation while trying to take advantage of AI; how it seeks to make AI satisfactory to all perspectives, unbound from governmental or business level but also civil society level (24).

November 2021: UNESCO Recommendation on the Ethics of Artificial Intelligence is adopted by its Member States

The Recommendation on the Ethics of Artificial Intelligence is the first global standard-setting instrument regarding AI, which consists of the aforementioned four core values and ten core principles. The four core values represent the basics of AI systems for the benefit of humanity, individuals, societies, and the environment, while the ten core principles represent the ethical standards of AI, with the focus on human rights (16). The Recommendation further emphasises data protection, as it bans privacy-breaching AI systems such as social scoring and mass surveillance and highly supports tools for assessing the impact of AI systems on individuals. In a practical aspect, the Recommendation initially obliges UNESCO to compose several tools, such as the Ethical Impact Assessment and Readiness Methodology. Then, the Member States are expected to implement them in their own nations and draft regular reports on their policies and executions (25).

November 2023: The Bletchley Park AI Safety Summit was held

The Bletchley Park AI Safety Summit was the first international AI summit, held in the United Kingdom (U.K.). The summit involved representatives with diverse perspectives, ranging from national leaders to representatives from industry and civil society. Its discussion centred around "frontier AI", which the U.K. defined as AI models that may exceed the capability of most existing models. The discussion addressed concerns and possible solutions, including developing tools to assess the potency of new AI models, establishing boundaries on the tolerable number of errors in AI, and debating the risks posed by AI models. The participants agreed that further collaborative action is necessary and emphasised the importance of inclusivity to ensure equitable development (26)(27). The consensus reached at the summit should serve as a constant reminder to the delegates that simply banning high-risk models and investing in safety mechanisms is insufficient.

August 2024: The European Union Artificial Intelligence (AI) Act comes into effect

The EU AI Act is the world's first overarching AI law aimed at enhancing EU citizens' experience, privacy, and safety with AI. The Act limits various entities and corporations when using AI for data sharing and collection. It classifies AI into four different categories: unacceptable-risk (those that violate people's rights and safety), high-risk (those used for disease diagnosis, automated cars, and biometric identification for investigation), limited-risk, and minimal-risk (ranging from AI-enabled games to chatbots). While limited-risk and minimal-risk-categorised models simply require transparency or have almost no regulations, high-risk models require stricter requirements and compliance measures, and unacceptable-risk models are completely banned from the EU. As it is the first law on AI, other regions, such as some states in the U.S., South Korea, and Brazil, have implemented similar laws (28)(29).

Position of key nations

The United States of America

The United States of America, one of the leading nations in the AI industry, recently declared that it will prioritise AI development over strict regulations. On January 23, 2025, President Trump issued Executive Order 14179, which promotes removing barriers to American leadership in AI. This led to modifying existing Federal regulatory frameworks in a way that promotes the adoption of AI applications. Though controversial, the nation still received trillions of dollars of investment from overseas. President Trump also declared that Congress should make a national standard with the least burden when it comes to AI regulations. The resulting new framework, as he claims, should therefore prevent all states from making separate state laws that would conflict with national laws, ensure child protection, prevent censorship, respect copyrights, and safeguard communities (30). The U.S. is also the first country to regulate AI by specifically putting export controls on it. On one hand, this allows the U.S. to export AI chips to allied nations without complying with AI regulations that limit the amount of chips exported. Meanwhile, on the other hand, the export control prevents the U.S. from exporting these AI chips to "countries of concern", where the term refers to countries that have U.S. arms embargoes, such as China (31).

China

China is also one of the leading nations in the AI industry, followed by large investments and a wide range of applications. Unlike the U.S., China shows more openness to AI regulations by introducing several AI-related policies involving AI regulations, industry standards, technical guidelines, and court rulings encompassing a wide range of AI models and cybersecurity. Meanwhile, China also shows proactive behaviour in AI usage. Its AI Plus Action Plan, established in 2025, covers how the country will strategise AI use in the future. The content consists largely of six fields where the nation plans to prioritise the deployment and development of AI in specific fields, some of them including consumer services and public welfare (32). China is also one of the countries that supports AI-enabled surveillance systems, as it recently launched the largest AI-based public-surveillance system and imposed an immense amount of workload that no other police officers had handled before. As much as AI is well-trusted to take a great stake in the government's national security, police officers now sit in command centres and monitor city security through this surveillance system. However, continuous development of AI models may trigger them to make final decisions, such as arresting, by itself without human command (33). Like China, many authoritarian regimes may value national sovereignty over human rights compared to democratic regimes. It is therefore important for Member States to fully consider and respect each other's priorities during discussions.

The United Kingdom

The United Kingdom, similar to the U.S., is more open to AI innovation and takes a more pro-innovation approach when it comes to AI regulation. Though the nation does believe that regulations are needed, it focuses more on maximising the benefit offered by AI and becoming a global leader in the field. The nation, therefore, takes a more encouraging and principles-based approach to its regulators, meaning that they lack comprehensive real-life action plans. For example, it relies on utilising existing regulators to regulate within their own sectors instead of establishing a new system and enforcing it. Because of this, the U.K.'s emphasis on regulators is often considered to be falling behind the EU. However, in 2025, a private members' bill in the House of Lords reissued the Artificial Intelligence (Regulation) Bill (AI Bill), which introduces a central AI Authority to monitor AI regulation, assess new AI risks, and support AI innovation while ensuring all innovation per sectors align with each other. Despite the Bill's significance it brings that will redirect the U.K.'s interaction with AI, the fact that the Bill is not yet issued by the U.K. government weakens its legal effectiveness (34)(35)(36).

Germany

Germany in the past was not strict in AI regulations and utilised soft laws that lacked legal enforcement. However, as a Member State of the EU, it is hence obliged to follow the AI Act. Though it still does not have a separate national law that regulates AI, the IT Law that addresses a wide range of technology issues also includes AI. It tackles liability, intellectual property, ethical compliance, sector-specific regulations, data protection and privacy (forcing AI systems to comply with the GDPR), and, most importantly, consumer protection. However, understanding that the nation might need further national laws, German politicians declared that they are constantly evaluating the necessity. While fully complying with the AI Act, Germany also focuses on its national prosperity. For instance, Germany adopted its National AI Strategy with a future goal of making Germany a global leader in AI through reinforcing the AI ecosystem, increasing both public and private sector uptake, while maintaining trustworthiness and sustainability in its AI developments. Though it may lack enforceable laws, Germany continues to maintain a balance between regulation and innovation (37)(38)(39).

South Korea

South Korea has recently established the world's second AI-specific legislation called the AI Basic Act, with a primary goal of fairly balancing between AI innovations and regulations. Coming into effect in January 2026, the Act is designed to reinforce national competitiveness through trusted development, ensure AI systems are deployed in an ethical manner, protect civilians from opaque systems, and support sustainable growth of the AI industry. Similar to the

GDPR, South Korea applies this law to any organisation that provides AI to its own citizens, widely affecting a large range of AI-related organisations (40)(41). Furthermore, instead of merely restricting AI, the Act also accelerates AI development through providing extra support to start-up companies, talent programmes, and industry clustering — a concentration of allied businesses (42). Though Korea has set legislative regulations on AI, it still sees AI as a chance for it to recover from recent economic instability. President Lee promised to donate 100 trillion won ($72 billion) as an investment to AI, increased the AI budget to 10.1 trillion won, and increased the AI Transformation initiative by 30% from last year. This portrays the capability of launching legally binding regulations while having grand visions on national prosperity (43), reminding Member States that if balanced right, economic growth and consumer protection can coexist.

Suggested solutions

AI has brought mankind numerous innovative solutions to current issues. Nowadays, most governments effectively utilise AI for national prosperity or sometimes for world power. Its ability to perform tasks goes beyond past thoughts, and still, humans continuously develop them to unlock its full potency. Although AI is helpful in various ways, its ability is sometimes abused or misused to cause harm to other civilians. Though it is hard to close the gap between the urgency for AI regulation and maintaining national prosperity, Member States should still remind themselves of the dire consequences AI will bring if not regulated strictly.

One main issue that should be addressed is that the world lacks a universal regulation or a framework. This allows some Member States the freedom to work with any type of AI system regardless of their risks. Therefore, one possible solution can be establishing a universal standard that categorises each AI technology in terms of its riskiness, where each of the categorised technologies will be regarded differently, similar to the EU AI Act. Having a common standard to start with will ease the excessive competition between nations by restricting them from experimenting with high-risk models. However, it would be challenging to get all nations to agree with the standards since there are nations that value national prosperity or leadership in the AI industry. For example, out of several international-level AI summits held in the past, the UN once launched a Global Dialogue on AI Governance, though the U.S. rejected it due to their preference for centralised control over its own AI policy (44). Likewise, these efforts to form multilateral regulations are constantly getting challenged due to varying perspectives.

Another possible solution can be gradually adding requirements when deploying or developing AI. Member States can start by requiring transparency on AI systems commonly exposed to consumers through notices that disclose information regarding the type of data the system will use, the use of collected data, and when AI is going to be used. Though it seems to be a small change, this will be a starting point for the world to decrease the risk of data misuse or leakage, one of the main issues that breaches consumer protection. Afterwards, nations can widely implement transparency mechanisms such as the HITL to ensure transparency in all systems, though it is not recommended to rely on HITL for too long since it has its own limits. As an alternative, while maintaining transparency with HITL, Member States are encouraged to find new transparency mechanisms with minimal side effects, which leads us to the next suggestion.

The next suggestion is to share technologies amongst nations. Developing new mechanisms or adopting new frameworks will cost a fair amount of money, and the level of burden on the cost may differ depending on each nation’s resource availability or economic situation. To ensure that

all consumers have guaranteed protection, it is thus important for Member States to have equal access to these resources and technologies. Sharing technology does not necessarily have to be free in cost, but reducing tariffs and trade barriers can be one strategy. Nations can also have experts to collaborate with each other or help train others for advanced technologies.

Nations are investing great effort into AI regulations, but consumer protection is still at risk. The most fundamental yet vital step is for all nations to come together and have a comprehensive action plan to make real-life changes, which many countries were deemed to lack. In addition to that, mandating AI systems to notify consumers on data collection and widely using existing practices or mechanisms for transparency may be seen as the simplest step to start with. Yet it is still significant, as these implementations will mark the start of the world moving in unison toward stronger protection. If Member States succeed in finding a midpoint of different perspectives and justly balance economic growth and consumer protection, civilians will be in a safer digital environment where AI provides maximum benefit to all.

Bibliography

1. Abdullah, Raja. “AI vs General Technology Differences - Raja Abdullah - Medium.” *Medium*, 21 Nov. 2024, medium.com/@rajaabdula16/ai-vs-general-technology-differences-b0042d70298d.
2. admin. “Why Is AI so Popular Now? The Key Factors behind Its Rise.” *SmartOSC*, 2 Apr. 2023, www.smartosc.com/why-is-ai-so-popular-now-the-key-factors/.
3. Pandey, Deepika. “The Importance of Artificial Intelligence in Everyday Life.” *Aeologic Blog*, 28 Mar. 2023, www.aeologic.com/blog/the-importance-of-artificial-intelligence/.
4. Gomstyn, Alice, and Alexandra Jonker. “Exploring Privacy Issues in the Age of AI.” *IBM*, 30 Sept. 2024, www.ibm.com/think/insights/ai-privacy.
5. “More than 50% of Fraud Involves the Use of Artificial Intelligence.” *Feedzai*, 2025, www.feedzai.com/inthenews/more-than-50-of-fraud-involves-the-use-of-artificial-intelligence/.
6. U.S. BUREAU OF LABOR STATISTICS. “Human Resources Managers : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics.” *Bls.gov*, 4 Sept. 2019, www.bls.gov/ooh/management/human-resources-managers.htm#tab-2.
7. Mesriani, Kadin. “AI & HR: Algorithmic Discrimination in the Workplace – Cornell Journal of Law and Public Policy.” *Cornell.edu*, 2024, publications.lawschool.cornell.edu/jlpp/2024/11/21/ai-hr-algorithmic-discrimination-in-the-workplace/.
8. Goettler, Peter. “Why AI Overregulation Could Kill the World’s next Tech Revolution.” *Cato Institute*, 3 Sept. 2025,

www.cato.org/commentary/why-ai-overregulation-could-kill-worlds-next-tech-revolution
.

9. "AI Surveillance and the Governance Vacuum in the Asia-Pacific | Lowy Institute." *Lowyinstitute.org*, 8 July 2025, www.lowyinstitute.org/the-interpreter/ai-surveillance-governance-vacuum-asia-pacific.
10. Ramanathan, Tara. "Artificial Intelligence Act | Framework, Applications, & Facts." *Encyclopedia Britannica*, 2 June 2025, www.britannica.com/topic/Artificial-Intelligence-Act.
11. Hyams, Joe. "Will Regulating AI Hinder Innovation?" *Trullion*, 17 May 2023, trullion.com/blog/ai-regulation/.
12. Huddleston, Jennifer. "AI and Privacy Rules Meant for Big Tech Could Hurt Small Businesses Most." *Cato Institute*, 20 May 2024, www.cato.org/commentary/ai-privacy-rules-meant-big-tech-could-hurt-small-businesses-most#:~:text=That's%20valid%20too;%20this%20cycle,consequences%20for%20startups%20and%20consumers.
13. Anglen, Jesse. "AI vs Traditional Software Solutions." *Kovench.com*, Rapid Innovation, 19 Sept. 2024, www.kovench.com/blog/ai-vs-traditional-software-solutions.
14. "Consumer Protection - Consumer-Protection." *Aseanconsumer.org*, aseanconsumer.org/cterms-consumer-protection/consumer-protection.
15. SAP. "What Is AI Ethics? The Role of Ethics in AI." *Sap.com*, 9 Aug. 2024, www.sap.com/resources/what-is-ai-ethics.

16. UNESCO. “Ethics of Artificial Intelligence.” *UNESCO*, www.unesco.org/en/artificial-intelligence/recommendation-ethics.
17. ASEAN. *ASEAN Guide on AI Governance and Ethics Contents*. 2 Feb. 2024, asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf.
18. Kosinski, Matthew. “What Is Black Box Artificial Intelligence (AI)?” *IBM*, 29 Oct. 2024, www.ibm.com/think/topics/black-box-ai.
19. Stryker, Cole. “Human in the Loop.” *Ibm.com*, 8 July 2025, www.ibm.com/think/topics/human-in-the-loop.
20. Wolford, Ben. “What Is GDPR, the Eu’s New Data Protection Law?” *GDPR.EU*, 2025, gdpr.eu/what-is-gdpr/.
21. OECD. “The OECD Artificial Intelligence (AI) Principles.” *Oecd.ai*, OECD, 2019, oecd.ai/en/ai-principles.
22. OECD. “OECD Updates AI Principles to Stay Abreast of Rapid Technological Developments.” *OECD*, 3 May 2024, www.oecd.org/en/about/news/press-releases/2024/05/oecd-updates-ai-principles-to-stay-abreast-of-rapid-technological-developments.html.
23. “About the Global Partnership on Artificial Intelligence (GPAI) - OECD.AI.” *Oecd.ai*, 2019, oecd.ai/en/about/about-gpai.
24. “Press Releases - 과학기술정보통신부 >.” *Msit.go.kr*, 2020, www.msit.go.kr/eng/bbs/view.do?sCode=eng&nttSeqNo=437&pageIndex=&searchTxt=&searchOpt=&bbsSeqNo=42&mId=4&mPid=2. Accessed 8 Mar. 2026.

25. ---. “UNESCO Adopts First Global Standard on the Ethics of Artificial Intelligence.” *Unesco.org*, 2021, www.unesco.org/en/articles/unesco-adopts-first-global-standard-ethics-artificial-intelligence.
26. Burki, Talha. “Crossing the Frontier: The First Global AI Safety Summit.” *The Lancet Digital Health*, vol. 6, no. 2, Elsevier BV, Jan. 2024, https://doi.org/10.1016/s2589-7500(24)00001-3.
27. “Chair’s Summary of the AI Safety Summit 2023, Bletchley Park.” *GOV.UK*, 2 Nov. 2023, www.gov.uk/government/publications/ai-safety-summit-2023-chairs-statement-2-november/chairs-summary-of-the-ai-safety-summit-2023-bletchley-park.
28. Ramanathan, Tara. “Artificial Intelligence Act | Framework, Applications, & Facts.” *Encyclopedia Britannica*, 2 June 2025, www.britannica.com/topic/Artificial-Intelligence-Act.
29. “Artificial Intelligence Act.” *Consilium*, 2020, www.consilium.europa.eu/en/policies/artificial-intelligence-act/. Accessed 8 Mar. 2026.
30. “Ensuring a National Policy Framework for Artificial Intelligence.” *The White House*, 11 Dec. 2025, www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.
31. The Regulatory Review, and Elizabeth Flatley. “The United States Regulates Artificial Intelligence with Export Controls | the Regulatory Review.” *The Regulatory Review*, 25

Sept. 2025, www.theregreview.org/2025/09/25/flatley-the-united-states-regulates-artificial-intelligence-with-export-controls/.

32. Li, Barbara. "Global AI Governance Law and Policy: China | IAPP." *IAPP.org*, 2025, iapp.org/resources/article/global-ai-governance-china.
33. Weber, Valentin. "China's AI-Powered Surveillance State." *DGAP*, 8 Oct. 2025, dgap.org/en/research/publications/chinas-ai-powered-surveillance-state.
34. Amin, Rosehana, and Adam Leese. "The Relaunched UK AI Regulation Bill – a Step towards Statutory Regulation of AI in the UK?" *Clydeco.com*, Clyde & Co LLP, 14 Mar. 2025, www.clydeco.com/en/insights/2025/03/the-relaunched-uk-ai-regulation-bill-a-step-toward.
35. "AI Regulation in the UK the Role of the Regulators - Bird & Bird." *Twobirds.com*, 15 Jan. 2026, www.twobirds.com/en/insights/2026/uk/ai-regulation-in-the-uk-the-role-of-the-regulators.
36. UK Government. "AI Regulation: A Pro-Innovation Approach." *GOV.UK*, 29 Mar. 2023, www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach.
37. horak. "AI Law as Part of IT Law in Germany | Horak Attorneys at Law: IT LAW EXPERTSIT Law, IT Contract Law, Data Protection Law, Media Law, Internet Law, IT License Law, IT Procurement Law, IT Outsourcing, Software Law, IT Projects Law, International IT Law, Open Source Law, Copyright Law, Compliance, Apps, SAAS, IP

Law, AI Law, Artificial Intelligence." *Horak Attorneys at Law: IT LAW EXPERTS ‣ IT Law, IT Contract Law, Data Protection Law, Media Law, Internet Law, IT License Law, IT Procurement Law, IT Outsourcing, Software Law, IT Projects Law, International IT Law, Open Source Law, Copyright Law, Compliance, Apps, SAAS, IP Law, AI Law, Artificial Intelligence*, 11 Mar. 2025, hitlaw.de/ai-law-as-part-of-it-law-in-germany/#page-content. Accessed 8 Mar. 2026.

38. "AI Regulatory Horizon Tracker - Germany." *Twobirds.com*, 2018, www.twobirds.com/en/capabilities/artificial-intelligence/ai-legal-services/ai-regulatory-horizon-tracker/germany.
39. Regulations.ai. "National AI Strategy — Update ('Fortschreibung Der KI-Strategie' / National AI Strategy: Update 2020)." *Regulations.ai*, 6 Jan. 2026, regulations.ai/regulations/RAI-DE-NA-NASUFXX-2020. Accessed 8 Mar. 2026.
40. "AI Regulation in South Korea: Complete Regulatory Guide." *Nemko.com*, 2024, digital.nemko.com/regulations/ai-regulation-in-south-korea.
41. "South Korean AI Basic Law | Artificial Intelligence Act." *Artificial Intelligence Act*, 2025, artificialintelligenceact.com/south-korean-ai-basic-law/.
42. "AI Basic Act of the Republic of Korea." *Aibasicact.kr*, 2025, aibasicact.kr/.
43. Park, Anna. "Korea Aims to Become Top 3 AI Power with New Presidential Committee." *The Korea Times*, 8 Sept. 2025, www.koreatimes.co.kr/southkorea/politics/20250908/korea-aims-to-become-top-3-ai-power-with-new-presidential-committee.

44. “How Is AI Changing the World?” *CFR Education from the Council on Foreign Relations*, 12 Mar. 2024, education.cfr.org/learn/learning-journey/how-ai-changing-world/regulating-ai.