Омбудсман України
Ombudsman of Ukraine

Фінансується Європейським Союзом

FIIAPP
COOPERACIÓN ESPAÑOLA

Ministry of Digital Transformation of Ukraine

HUMAN RIGHTS IN THE ERA OF ARTIFICIAL INTELLIGENCE

CHALLENGES AND LEGAL REGULATION

2024

Human rights in the era of Artificial Intelligence: challenges and legal regulation is a methodical document that discusses the impact of cutting-edge artificial intelligence technologies on human rights and approaches to its legal regulation. It also offers recommendations on managing the intellectual system in accordance with national legislation and international standards.

The publication was developed within the framework of the international project EU4DigitalUA in collaboration with the Office of the Ombudsman and the Ministry of Digital Transformation of Ukraine.

Participation in the preparation of the publication:

Ulyana Shadska
Andrii Nikolaev, Yulia Derkachenko, Volodymyr Begei, Gordiy Rumyantsev, Oleg Dubno, Oleksandr Marchenko

The EU4DigitalUA project is part of the European Union's support for Ukraine. The views, thoughts and conclusions expressed in the text belong solely to the authors and do not necessarily represent the position of the project, the European Union, or FIIAPP.

Омбудсман України
Ombudsman of Ukraine

Фінансується Європейським Союзом

FIIAPP
COOPERACIÓN ESPAÑOLA

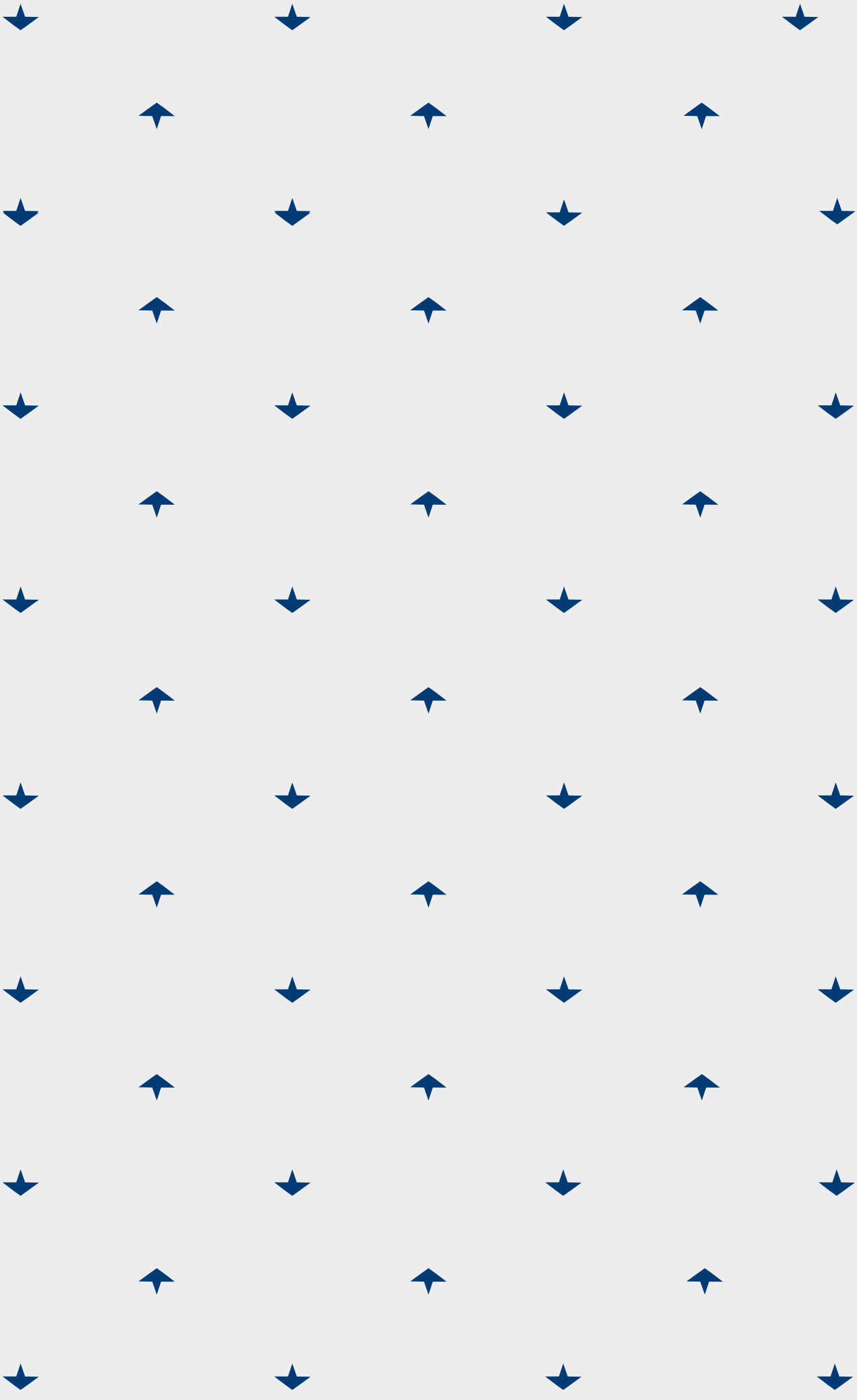
Ministry of Digital Transformation of Ukraine

HUMAN RIGHTS IN THE ERA OF ARTIFICIAL INTELLIGENCE

CHALLENGES AND LEGAL REGULATION

2024

INDEX



INTRODUCTION

Today, artificial intelligence is used in almost all spheres of human activity. Cutting-edge technologies can perform a diverse range of tasks: managing vehicles, production processes within enterprises, generating text, music, recognising faces and voices, serving as personal assistants on smartphones, and much more. They are integrated into various devices used daily in government policies, urban infrastructure, business, or simply in everyday life. Despite the broad societal prospects that intelligent systems can create, attention must also be directed towards the ethical and legal aspects of their usage, particularly their impact on human rights and freedoms.

One of the most serious risks involves the violation of the right to privacy.[1] Improper or erroneous use of confidential information about an individual in artificial intelligence systems can lead to negative consequences for them. This is especially the case when it concerns data such as an individual's health, gender, ethnicity, biometric data, and so on. This applies both to the very essence of the technologies and the specific ways in which they are applied, which can result in challenges when contesting automated decisions, biases or discrimination. These aspects are often interconnected.

Stakeholders involved in the lifecycle of artificial intelligence systems, including those organisations or individuals developing, deploying or using them, must implement organisational and technical measures to ensure the safe operation of such technologies in compliance with legislation and international standards. A comprehensive programme for managing the intelligent system is needed, involving an in-depth analysis of its operations, particularly regarding its impact on human rights and freedoms. As practical experience shows, this can be a challenging task, as it requires understanding not only the essence of such technologies and their usage parameters but also the social and legal contexts.

In this regard, as part of the international initiative EU4DigitalUA in collaboration with the Office of the Ombudsman and the Ministry of Digital Transformation of Ukraine, a methodical document has been prepared. It elucidates the general aspects of the impact of artificial intelligence and approaches to its legal regulation, especially in personal data processing. Striking a balance between technological advancement and the protection of human rights is extremely crucial, as the future of society hinges upon this equilibrium.

This material is based on the provisions of national and international legislation, documents from the Council of Europe, the Organization for Economic Co-operation and Development (OECD), the United Nations, including UNESCO's recommendations on the ethical aspects of artificial intelligence. It takes into account practices and clarifications from supervisory bodies in this field,

1 Over 57% of consumers consider the use of artificial intelligence in collecting and processing personal data as a significant threat to their confidentiality, according to a study by the International Association of Privacy Professionals (IAPP) in 2023.

including the Spanish Data Protection Agency (AEPD), the Information Commissioner's Office in the UK (ICO), the French National Commission on Informatics and Liberties (CNIL), and others. Additionally, expert opinions, comments and recommendations from the Ukrainian Parliament Commissioner for Human Rights, the Ministry of Digital Transformation of Ukraine, other government bodies and Ukrainian civil society organisations have been considered.

1. CONCEPT AND ROLE OF ARTIFICIAL INTELLIGENCE IN MODERN SOCIETY

In December 2020, the Cabinet of Ministers of Ukraine approved[2] the Concept for the Development of Artificial Intelligence in Ukraine, which defines the goals, principles and tasks for the development of such technologies as one of the priority directions in the field of scientific and technological research.

The Concept defines the terms as follows:

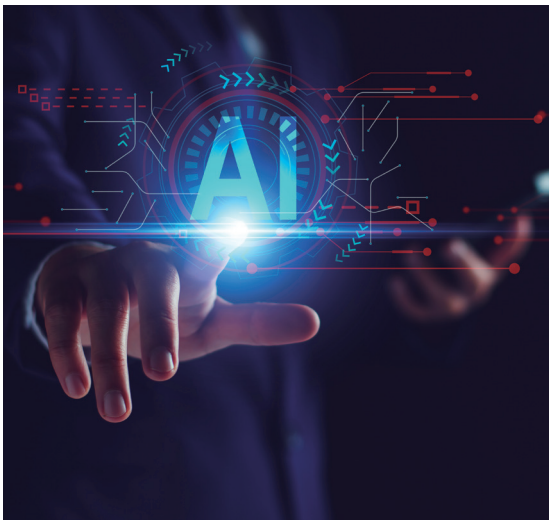
Artificial Intelligence (hereinafter referred to as AI technologies) — an organised set of information technologies, employing which complex tasks can be performed through the application of a system of scientific research methods and information processing algorithms, utilising information obtained or independently created during work. It also involves creating and utilising proprietary knowledge bases, decision-making models, information processing algorithms and determining methods to achieve set tasks.

The field of artificial intelligence — a direction of activity in the field of information technologies that ensures the creation, implementation and use of AI technologies.

In the European Parliament, AI is defined as any tool used by a program to replicate human-associated behaviours, such as reasoning, planning, and creativity. This concept can be broadened, as AI is already capable of exceeding human capabilities.[3]

AI stakeholders — includes all those involved in the life cycle of the system, including organisations and individuals deploying or managing AI.

Interested parties — institutions, organisations, as well as private individuals directly or indirectly involved in the AI system.[4]



2 The Cabinet of Ministers of Ukraine adopted the decree "On Approval of the Concept for the Development of Artificial Intelligence in Ukraine."

3 Intelligence artificielle : définition et utilisation: https://www.europarl.europa.eu/news/fr/headlines/society/20200827STO85804/intelligence-artificielle-definition-et-utilisation

4 OECD, Recommendation of the Council on Artificial Intelligence.

1.1. AREAS OF APPLICATION OF ARTIFICIAL INTELLIGENCE

The field of Artificial Intelligence (AI) is advancing rapidly across various sectors. Medical institutions and research centres utilise AI for disease diagnosis, studying medical data and developing personalised treatment approaches. Law enforcement agencies implement AI technologies to ensure public safety, and to forecast, prevent and investigate crimes. For instance, analysing extensive data from surveillance cameras, social networks and phone calls helps identify patterns and anomalies that may indicate potential criminal activities or threats to national security.

Additionally, banking and other financial institutions use AI programs to provide services, analyse economic indicators, process payments and prevent fraud. In the business sphere, AI helps in automating routine tasks such as order processing, production management and market demand analysis. Various companies and services like Netflix, YouTube, Amazon, widely used by Ukrainians, use AI to process customer information, including their online behaviour, to create marketing programs.

In the education sector, AI is applied to develop individualised learning approaches, assess knowledge and create interactive platforms. As stated on the official website of the Ministry of Digital Transformation of Ukraine: "Data is the new oil, artificial intelligence is the new electricity" — these are the realities of the modern world.[5]

1.2. THE IMPACT OF ARTIFICIAL INTELLIGENCE ON HUMAN RIGHTS

Despite the broad prospects modern AI technologies offer to society, some of them can significantly impact fundamental human rights and freedoms. Firstly, AI can make mistakes. There are already sufficient precedents worldwide that demonstrate this fact.

For example, among prominent cases is the scandal in the UK[6] between 2000 and 2014 when over 700 postal service workers were penalised, with some even imprisoned, for offences they did not commit. The company's computer program flagged financial discrepancies, leading to the accountability of many employees. It took years for lawyers to prove that the system had made an error. Other potential risks in algorithm operations have been demonstrated by scientists. The University of Essex, in its research, concluded that the error rate in the British police's video surveillance system and facial recognition was 81%.[7] The program could identify four innocent individuals out of five as suspects. Similar findings were also published in a report by the Georgetown Law Center on Privacy and Technology.[8]

Secondly, the operation of intelligent systems may involve the processing of personal data, posing a risk of violating the right to privacy. In January 2020, discussions arose among the public in various countries, including Ukraine,[9] regarding Clearview AI, a company developing facial recognition technologies. Its system operates using AI and machine learning to collect and analyse a

5 The Ministry of Digital Transformation has formed an expert committee on the development of the artificial intelligence sphere: https://thedigital.gov.ua/news/mintsifra-sformuvala-ekspertniy-komitet-z-pitan-rozvitku-sferi-shtuchnogo-intelektu

6 Post Office scandal: What the Horizon saga is all about: https://www.bbc.com/news/business-56718036

7 UK police's facial recognition system has an 81 percent error rate: https://www.engadget.com/2019-07-04-uk-met-facial-recognition-failure-rate.html?guce_referrer=aHR0cHM6Ly93d3cuZ2gvZ2xlLmNvbS8&guce_referrer_sig=AQAAAJC6imMAdnNgJ17SdmSfPn2zYD8McbsmvwIPrmjdfchxnLKvE1PwtQd9GHbVyMLxc-puxTLEAVeKSCIKf3DFtlU2EF4g7i9yQK9aIYiV_3WkX2q-3DcHfJklyw-AwHWNZPupTIouU_uC3JeTaBHZ3_DtKL45scBzwqD4CqG3w3KM&utm_campaign=AI+Weekly&utm_medium=email&utm_source=Revue+newsletter&guccounter=1

8 Garbage in, garbage out. Face recognition on flawed data: https://www.flawedfacedata.com/?utm_campaign=AI%20Weekly&utm_medium=email&utm_source=Revue%20newsletter

9 Ukraine gained access to the database of the Clearview AI facial recognition system: https://zaxid.net/ukrayina_otrimala_dostup_do_bazi_sistemi_rozpiznavannya_oblich_clearview_ai_n1538330.

vast number of images of individuals obtained from the internet. Clearview AI claimed its product could identify individuals from real-time photos by comparing them to images in its database collected from open internet sources such as social networks, news websites and other publicly available resources.

The issue lies in the fact that this company collects personal data of individuals without their consent, raising concerns about the legality of such actions. In the US, a class-action lawsuit was filed against Clearview AI, accusing the company of selling biometric data to law enforcement agencies.[10]

Additionally, the activities of this company have been banned in some European countries. However, it continues to provide its services worldwide. The controversial nature of this issue sparks numerous discussions that push legal fields to find a balance between the benefits of technology and its risks.

These issues can concern both the essence of AI technologies and the specific ways they are applied. It may be associated with the lack of transparency in system development and operation, risks of bias and discrimination, and the complexity of challenging automated decisions. These aspects are often interconnected.[11]

Due to insufficient transparency in AI algorithms, situations may arise when individuals whose rights have been affected by the actions or decisions of the system are unaware of the reasons behind these occurrences. This includes instances where individuals have been denied certain services or subjected to specific decisions without understanding the reason why. For example, Amazon used AI to review resumes for job vacancies, only to later discover that the program was rejecting all applications based on gender-related patterns.[12] Another resonant scandal involved citizens' access to social benefits in the Netherlands. Under the Ministry of Social Affairs and Employment in the Netherlands, several cities started using the System Risk Indication (SyRI) to detect welfare fraud. During the risk analysis for fraud, SyRI processed the data of welfare recipients.[13] It was later revealed that the risk assessment in the sector involving individuals with lower incomes was uneven, causing societal outrage and accusations of discrimination against the government, as potential beneficiaries were unable to comprehend the decision-making mechanisms of this system. In 2020, a Dutch court

10 In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois: https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois

11 Rodriguez, 2020.

12 Amazon built an AI tool to hire people but had to shut it down because it was discriminating against women: https://www.businessinsider.com/amazon-built-ai-to-hire-people-discriminated-against-women-2018-10

13 How Dutch activists got an invasive fraud detection algorithm banned: https://algorithmwatch.org/en/syri-netherlands-algorithm/

deemed the use of the current version of SyRI illegal, citing violations of the right to private and family life under Article 8 of the European Convention on Human Rights. The court highlighted the opacity of the system, which collected an excessive amount of personal data without specific purposes.

Currently, in Ukraine, there is limited research on similar cases, but this does not imply their absence. It can be said that the work being done in this direction has only just begun. This publication aims to draw attention to the necessity of taking measures to explore potential issues related to the use of AI in both the private and public sectors.

As stated in the Concept of Artificial Intelligence Development in Ukraine, the implementation of information technologies is an important component of socio-economic, scientific-technical, defence and other activities. Specifically, Ukraine aims to occupy a significant segment of the global AI technology market and attain leading positions in international rankings. However, the absence of conceptual principles in state policy in this field hinders the creation and development of a competitive environment. This underscores the need to address issues such as:

- Low level of investment in AI research at higher education institutions.
- Inadequate publications in leading industry conferences and prominent peer-reviewed publications.
- Imperfect mechanisms for making managerial decisions in the public sphere, bureaucratic complexities affecting the provision of administrative services, limited access to information and its low quality, insufficient implementation of electronic document circulation among government bodies and a low degree of data digitalisation owned by government entities.
- Complexity in verifying compliance of AI systems with legislation and ethical principles.
- Lack of unified approaches in defining ethical criteria during the development and use of AI technologies for different industries, activities and sectors of the national economy.
- Risks of increased unemployment due to the use of AI technology.
- Low level of digital literacy and of public awareness regarding general aspects, possibilities, risks and security inherent to AI use.
- Insufficient information security and data protection in the information-telecommunication systems of government bodies due to outdated automatic threat detection and evaluation systems, underutilisation of forecasting potential and prediction of threats for timely system preparation against possible attacks.
- Increased attempts to carry out unauthorised interventions in the functioning of automated systems and computer networks.
- Absence or imperfection in the legal regulation of AI (including in education, economy, public administration, cybersecurity, defence), as well as inadequacies in legislation regarding personal data protection.

It is evident that AI technologies will continue to evolve, expanding their capabilities in various spheres. Therefore, it is crucial to analyse their impact on human rights and freedoms and to establish ethical and legal frameworks.

2. LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE

Ukraine is a member of the Committee on Artificial Intelligence at the Council of Europe and participates in the Working Group on AI Governance at the Organization for Economic Cooperation and Development (OECD). In November 2023, during the AI Safety Summit held in the United Kingdom, Ukraine signed the "Bretton Woods Declaration" and thus joined international cooperation in researching AI safety. According to this document, participating states must collaborate to mitigate AI risks and promote its design, development and use in a safe manner. This pertains both to public services across various sectors and to business operations.

In the Concept of Artificial Intelligence Development in Ukraine, certain principles are outlined, including:

- Development and utilisation of AI systems only under the condition of upholding the rule of law, fundamental human and citizen rights and freedoms, democratic values, and ensuring appropriate guarantees during the use of such technologies.
- Compliance of AI system activities and decision algorithms with legislation on personal data protection, as well as adherence to the constitutional right of each individual to non-interference in personal and family life regarding personal data processing.
- Ensuring transparency and responsible disclosure of information about AI systems.
- Reliable and secure functioning of AI systems throughout their lifecycle and continuous assessment and management of potential risks.
- Imposing responsibility on organisations and individuals involved in developing, implementing or using AI systems for their proper functioning in accordance with the specified principles.

Considering that the operation of AI technologies often involves the processing of personal data, such activities fall under the scope of relevant legislation. The existing Ukrainian Law "On Personal Data Protection" does not account for the specifics of AI operations. However, Ukraine is a party to international agreements and other regulatory documents ratified by the Verkhovna Rada of Ukraine. Particularly, the Association Agreement between the EU and Ukraine, effective from September 2017, includes obligations to ensure personal data protection in line with European and international standards, as outlined in Article 15 of the Agreement.

This entails that international requirements must be considered during the development and application of such technologies. Additionally, numerous Ukrainian AI programs process personal data of individuals residing in EU countries, making them subject to the General Data Protection Regulation (GDPR) regulation. This also pertains to the international standard ISO/IEC 27701:2019, which extends the requirements of ISO/IEC 27001 and 27002 standards regarding information security and information protection, specifically during identification using Personally Identifiable Information (PII). It includes the IEEE P7003™ standard developed by the IEEE to address specific challenges related to AI, focusing on identifying and mitigating biases in AI algorithms, particularly during the processing of sensitive data. Moreover,

it encompasses provisions from the Council of Europe, the United Nations, the European Court of Human Rights protected by the international human rights system. On 18 December 2023, the International Organization for Standardization (ISO) published a new standard ISO/IEC 42001:2023 containing requirements for establishing, implementing, supporting and continually improving AI systems. The provisions of this standard are applicable to any institutions or organisations, regardless of their field of activity.[14]

At the same time, it is essential to note that the Declaration on Ethics and Data Protection in Artificial Intelligence establishes a connection between the collection, use of personal information, and AI development.[15] This connection necessitates the following clarifications:

1. Personal data constitutes a legal category of information with specific rules to be followed in AI project development.
2. Not every AI system involves processing personal data.
3. Personal data is not the sole form of information collected, stored, analysed or used in the development of AI.

In Ukraine, the process of developing AI legal regulation has only just begun. The Ministry of Digital Transformation of Ukraine has published a Roadmap for regulating artificial intelligence in Ukraine. This is based on a bottom-up approach aimed at providing practical business tools, such as regulatory sandboxes, methodologies for assessing the impact of AI on human rights and tools for labelling AI systems, among others.

Most countries also lack specific AI laws. China stands as an exception with its temporary measures governing AI generative services, effective from August 2023.[16] This document aims to ensure that generative AI aligns with "social order and morality", remains accurate, avoids discrimination, and upholds intellectual property rights. Singapore's National AI Strategy comprises a Model AI Governance Framework, highlighting practical aspects of AI governance at the organisational level.[17] Canada's AI and Data legislation, as part of Bill C-27, is also under refinement. In the USA, federal policies on AI management have been established.[18] Within the European Union, there is the development of a new comprehensive Regulation on Artificial Intelligence, scheduled for official adoption in 2024, including a transitional period for implementation by AI stakeholders.

Understanding the global legal context is crucial because in most cases, AI technologies have a transnational impact and require a balance between innovation and ethics, technology and human rights. A deep understanding of these interrelations will enable the creation of an effective legislative framework for Ukraine.

14 ISO/IEC 42001 is an international standard that specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organisations: https://www.iso.org/standard/81230.html

15 Cfr. "Declaration on ethics and data protection in artificial intelligence". 40th International Conference of Data Protection and Privacy Commissioners. Tuesday, 23rd October 2018, Brussels.

16 Temporary measures to manage artificial intelligence generative services: https://www.chinalawtranslate.com/generative-ai-interim/

17 National Artificial Intelligence Strategy: https://www.smartnation.gov.sg/initiatives/artificial-intelligence/

18 The Artificial Intelligence and Data Act (AIDA) — Companion document: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

2.1. APPROACH TO LEGAL REGULATION IN THE EU COUNTRIES

In the European Union, provisions are being developed to regulate the use of information technologies. Specifically, these pertain to confidentiality in electronic communications, delineating which GDPR provisions will apply to protect data on the internet. This document could have significant implications for AI entities offering electronic communication services. Next are the Digital Markets Act (DMA), Digital Services Act (DSA) and Data Governance Act (DGA). In 2023, the European Parliament adopted the draft Regulation on AI regulation (referred to as the AI Act), a concept proposed by the European Commission back in April 2021. These provisions aim to create a common legal framework for anyone developing or utilising AI systems in EU countries and beyond. It is intended to serve as an example of unifying legal rules in the field of AI.[19]

19 Artificial Intelligence Act: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

A brief chronology and upcoming legislative changes in the EU[20]:

April 2021	The European Commission presented its proposal for an Artificial Intelligence Regulation.
December 2022	The European Council adopted a common position (common approach) on the Artificial Intelligence Regulation.21
June 2023	MEPs adopted their position on the Artificial Intelligence Regulation.
End of 2023	Political agreement was reached on the provisions of the Artificial Intelligence Regulation.
Start of 2024	The final version of the Artificial Intelligence Regulation is expected to be adopted.
End of 2025 — beginning of 2026	The EU Artificial Intelligence Regulation is expected to enter into force after a likely 18-24 month transition period.

Around the AI Act, many discussions ensue. On one hand, opinions suggest that such a law should restrict the application of certain AI technologies that may pose a danger to human rights and freedoms. On the other hand, there is an assertion that such an act might hinder innovation and societal progress overall. Despite these discussions, all sides agree that AI technologies require legal regulation. Experts from the NGO "Center for Democracy and Rule of Law" analysed[22] the new AI Act, highlighting important aspects worth noting. Particularly, the new Regulation in the EU:

- Will require a risk management system throughout the entire life cycle of AI, not just during development.
- Introduces mandatory certification for certain AI systems, especially those processing special categories of data, conducting large-scale profiling of individuals, educational or professional evaluation systems, or critical infrastructure.
- Contains provisions for datasets that must be current, complete, error-free and have appropriate statistical characteristics. This condition aims to reduce potential biases in systems and the number of discriminatory decisions.
- Imposes limitations on systems that may potentially risk human rights or state interests. For instance, this concerns issues of discrimination, misinformation and other manipulations in the information space.
- Establishes requirements for certain AI systems regarding the necessity to inform users that they are interacting with an AI system, not a human.
- Demands assistance in developing Codes of Conduct for AI subjects based on the intended purposes of respective systems.
- Emphasises the need for transparency in the development and use of AI systems.
- Creates specialised regulatory sandboxes.
- The concept of regulatory sandboxes is one of the innovative measures proposed by the AI Act, aimed at facilitating the implementation of AI systems in practice.

Thus, AI regulation in EU countries is based on a risk-oriented approach, also proposed in the White Paper on Artificial Intelligence in 2020.[23] However, at that time, only two risk levels were described, and later, this issue was further examined, forming four levels:

- AI systems with minimal risk or non-risky.
- AI systems with limited risk.
- AI systems with a high degree of risk.
- Prohibited AI systems.

20 Contentious areas in the EU AI Act trilogues: https://iapp.org/news/a/contentious-areas-in-the-eu-ai-act-trilogues/

21 Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights. Режим доступу: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

22 Olga Petriv, Artificial Intelligence and the AI Act: Time for Legal Frameworks: https://cedem.org.ua/analytics/artificial-intelligence-act/

23 Commission White Paper on Artificial Intelligence: A European approach to excellence and trust, COM (2020) 65 final (February 19, 2020).

The minimum risk is characterised by a low impact on the rights and freedoms of individuals. This may involve using AI for automating routine tasks that do not have significant legal consequences, such as document processing or generating standard letters or messages. At the level of limited risk, AI may affect the rights and freedoms of individuals, but this can be controlled and regulated. Users of such AI should be aware that they are interacting with a machine and make their decisions as to whether to continue or terminate the interaction.

A high level of risk indicates the potential for a serious impact on the rights, freedoms and interests of individuals. Applying AI at this level usually involves making automated decisions that may have legal consequences. Such AI systems must comply with mandatory requirements and undergo conformity assessment procedures before entering the EU market. Clear obligations are placed on providers and users of these systems, including:

- Clear and adequate information about the operation of this technology.
- Applying human intervention measures to minimise the risks of rights infringements.
- Registering activities to ensure traceability of results.
- High-quality datasets feeding the system to minimise discrimination risks.
- Detailed documentation providing all necessary information about the system and its purpose.
- Ensuring adequate risk assessment and mitigation systems.
- Ensuring a high level of reliability, security and accuracy.[24]

Prohibited AI technologies include those posing a threat to individuals or society as a whole. For example, using such programs for tracking, manipulation, propaganda or for use against vulnerable social groups, among others.

Each of these risk categories has subcategories. The initial list proposed by the European Commission has been reviewed by both the European Council and Parliament. In their amendments, the European Parliament added to the classification high-risk AI systems that use certain social media platforms (i.e., those marked as "very large online platforms" according to the Digital Services Act) to create recommendations for users, especially those AI systems capable of influencing election outcomes or other democratic processes in states.[25]

The risk classification allows developers or users of AI to identify situations in which such technology could cause harm. Overall, the architecture of the AI Act's enforcement resembles the GDPR, and this parallel becomes even more relevant, considering that some national data protection institutions, such as France's National Commission on Informatics and Liberty (CNIL), are already positioning themselves as supervisory authorities in the field of AI.

Therefore, if the EU achieves its goal in the near future—adopting the final version of the AI Act—it is expected to come into effect no earlier than 2026 and will be active for a certain period during which stakeholders can adapt their operations to comply with its provisions. The adoption of the AI Act will directly impact the regulation of AI in Ukraine, entailing the need to start working on mechanisms for implementing and incorporating international standards into Ukrainian technological projects.

24 Artificial Intelligence and the Artificial Intelligence Act: Time for Legal Frameworks: https://cedem.org.ua/analytics/artificial-intelligence-act/

25 Contentious areas in the EU AI Act trilogues: https://iapp.org/news/a/contentious-areas-in-the-eu-ai-act-trilogues/

2.2. APPROACH TO LEGAL REGULATION IN THE USA

In the United States, there is an active development of federal policies regarding AI. There are various initiatives, laws and policies aimed at assessing risks and regulating AI operations. A foundational strategy has been crafted, providing a general idea of legal and political approaches to regulating new technologies. The White House Office of Science and Technology Policy (OSTP) published[26] the Concept of the Artificial Intelligence Law, emphasising the importance of technological development while expressing concerns about its impact on human rights and freedoms, particularly regarding digital surveillance and profiling. To address these concerns, five levels of protection have been proposed in the US:

1. Protection against dangerous or ineffective systems.
2. Protection against digital discrimination.
3. Protection of personal data and prevention of excessive intrusion into people's private lives.
4. Transparency in the use of AI technologies, specifically their potential impact on human rights and the environment.
5. Protection against automated decision-making.

During the development of this concept, various questions were considered:

- What should developers of AI do to prioritise human rights at the inception of technology design?
- How can AI technologies and other innovations be used ethically?

26 Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/

The Concept presents a vision for a society where the protection of human rights aligns with technological progress. It integrates input from diverse social groups, reflecting the need for clear legal regulations for AI and state guarantees of protection in case of risks. The document includes a technical appendix outlining specific steps that communities, government bodies and other stakeholders can take to implement key protective principles against the negative impacts of AI.

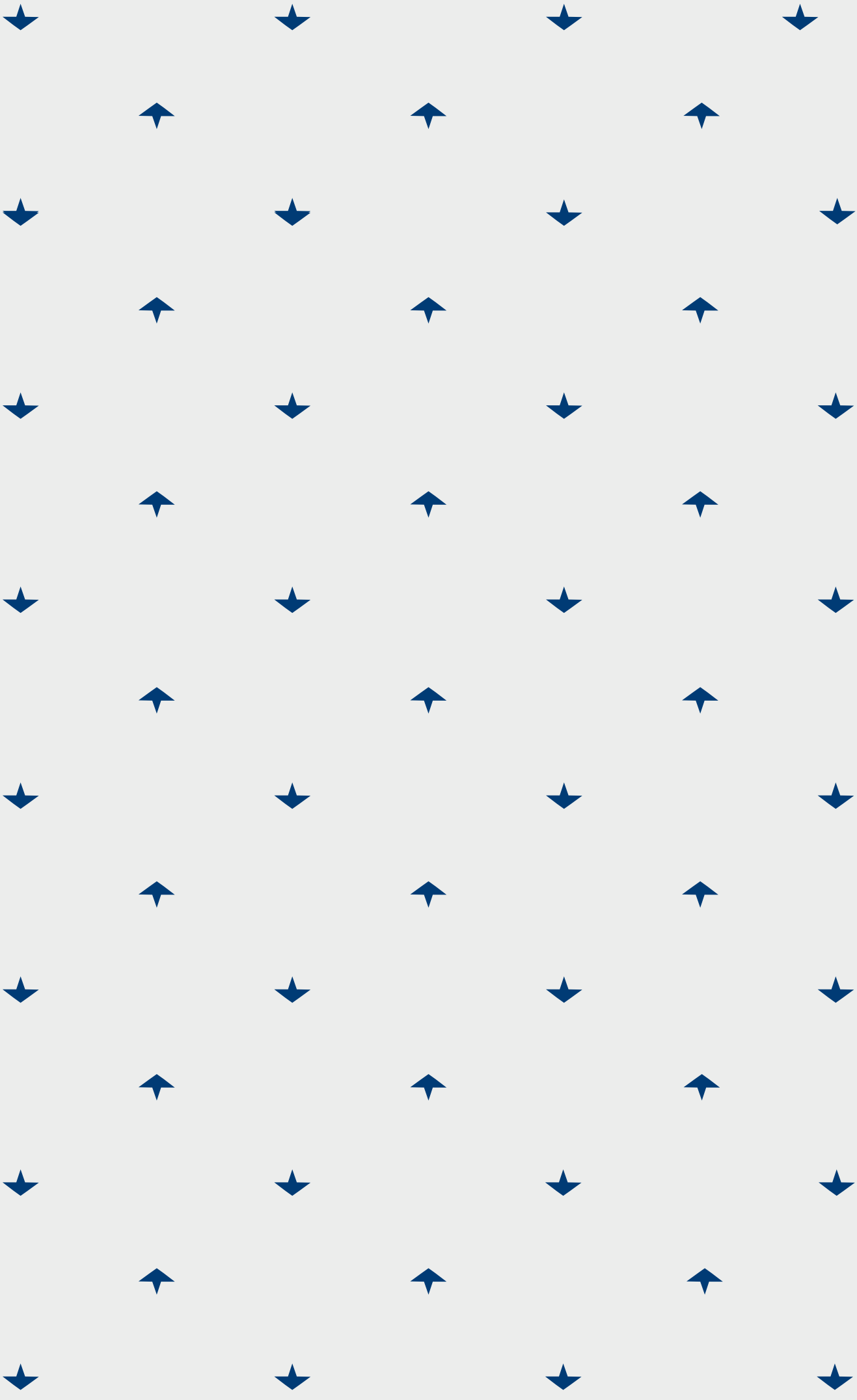
According to the Concept, several key aspects have been highlighted:

1. **Transparency and Understandability.** Individuals have the right to know when and how AI is being used. They should have access to understandable information about its principles of operation.
2. **Prevention of Discrimination.** AI systems must be developed and used to prevent any forms of discrimination based on race, gender, religion, sexual orientation and other characteristics.
3. **Privacy Protection.** People have the right to control their data collected and used by AI technologies. Laws regulating each sector should include requirements for monitoring and using AI, embedding by default principles and standards that protect individuals' privacy. Proposed reinforcement includes protecting sensitive data related to health, employment, education, criminal justice, finances and youth.
4. **Responsibility and Accountability.** Entities creating or using AI systems should be accountable for their actions and potential consequences. Technologies should evolve under enhanced control, with effective risk assessment and adherence to ethical frameworks. People should be protected from automated decision-making that might restrict their rights and freedoms. The Concept includes a reporting system from developers or users, particularly when collecting and processing personal data. These reports should be in an understandable form, assessing not only the usage of such systems but also their impact on human rights.
5. **Right to Protection from Automated Decision-Making.** If individuals face negative consequences due to decisions made by AI systems, they have the right to challenge and rectify them. If a machine makes a decision affecting a person, that result should be reviewed and monitored.

The Concept also emphasises that the technical capabilities of AI are evolving rapidly, implying that potential harm can arise even from programs which are seemingly less developed. It proposes a two-stage test to determine which systems fall under the scope of the document: (1) automated systems that (2) could significantly impact the rights, opportunities or access of citizens to key resources or services.[27] Thus, it can be concluded that the US approach to regulating AI systems aligns with international standards and principles recognised and applied in other countries worldwide, particularly in the EU.

Therefore, studying the experience of other countries in regulating AI technologies is an important task. Ukraine, along with other legal and democratic states, should strive for unified standards in protecting human rights and freedoms amidst technological development and cyberspace in general. Knowledge of international principles and regulations regarding AI can contribute to creating an environment for scientific research and the integration of Ukrainian developments into the global market.

27 Data privacy. You should be protected from abusive data practices via built-in protections, and you should have agency over how data about you is used: https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/



3. INTERNATIONAL PRINCIPLES

Various international provisions propose a series of principles that form widely accepted standards for the development and legal regulation of AI technologies.[28] For instance, the international group of experts from the European Commission published an ethics guide for trustworthy artificial intelligence. This guide establishes conceptual rules for AI operation depending on the context of its use. Specifically, it addresses:

a. **Legality.** Adherence to all laws and regulations defined in international and national provisions.
b. **Ethics and Responsibility.** AI operations should align with ethical principles and values of both local and global communities.
c. **Reliability.** AI systems must be reliable and safe for humans.

According to Virginia Dignum,[29] an associate professor of engineering systems and services at Umeå University, as advances in machine learning allow AI to autonomously make decisions without direct human control, there should be a push for the concept of ethical and responsible AI at all levels.

This concept should include:

a. **Transparency and Accountability.** The necessity to explain and justify decisions regarding the development and usage of AI that affect human rights and freedoms.
b. **Responsibility and Human Oversight.** Humans should have roles in identifying errors or illegitimate outcomes.

Here we will delve into several principles mentioned in international documents and practices.

28 The report by the Special Rapporteur of the United Nations General Assembly on the Right to Privacy, Joseph A. Cannataci, is titled «Artificial Intelligence and the Right to Privacy, as well as the Right to Privacy of Children.»

29 The ART of AIDesign — Accountability, Responsibility, Transparency: https://www.delftdesignforvalues.nl/2018/the-art-of-ai-accountability-responsibility-transparency/

TRANSPARENCY

Transparency involves describing and verifying the mechanisms through which AI systems make decisions. In the context of AI, transparency is crucial as it fosters trust in these technologies. Understanding how and why a system arrived at a particular decision is important for ensuring reliability and predictability, especially in areas using automated decision-making systems. Thus, ensuring transparency positively impacts the validation and certification of AI systems. For instance, in cases where a system decides on granting subsidies or loans, it is vital to comprehend the evaluation criteria used and whether they comply with legal requirements.

Legislative frameworks may require organisations to adopt transparent and understandable AI models. In legal proceedings against an organisation, transparency in their AI systems aids in clearly explaining how their technology works and why it made specific decisions. This can facilitate the ability to take preventive measures if necessary.

Therefore, providing timely and understandable notifications about the use of AI systems is crucial. Users should receive advance notifications about the use of automated systems. Explanations should be available alongside the decision or shortly afterwards. Notifications and explanations can be in various formats.[30]

One of the documents demanding this principle in the operation of AI systems is the "Ethical Guidelines for Trustworthy AI" developed by the European Commission.[31] It provides recommendations for qualitative and quantitative metrics to evaluate the transparency of AI systems. Additionally, it is important to consider the concept of the right to explanation, where individuals have the right to know how an AI system reached a decision that could affect their rights and interests.

It is possible that absolute transparency may be unattainable due to the functionality of specific systems, certain algorithmic details might be restricted due to intellectual property or state secrets. However, this does not negate the need to explain how AI operates, albeit only to a specific group, such as regulatory bodies in the field. Transparency, in the context of this principle, focuses on disclosing information about AI usage. It does not entail disclosing commercially or legally protected secrets. It means society should have general information on how AI is used in a particular field to make informed choices and mitigate potential risks. Another aspect of transparency relates to public consultations and increasing public awareness of AI operations. Such an approach should be supported in a society founded on laws that prioritises human rights and freedoms.[32]

If AI systems process personal data, explaining the data processing process is a legal requirement. Processing personal data should occur openly and transparently, using means and methods that align with defined purposes. Transparency ensures that everyone receives information about the processing of their personal data and direct access to them. Individuals should be aware not only of the potential benefits but also of the risks associated with the application of AI systems. The data owner must explain in an accessible format to the general public how and why they obtain the data, how they plan to use them, and to whom they might transfer them.

Looking at recommendations from state regulators in EU countries, the demand for transparency in processing personal data by AI systems holds a central place. In their assessments, questions are posed to AI stakeholders about how transparency in technology usage is ensured. For example, the UK Information Commissioner's Office (ICO) focuses on:

30 Information Commissioner's Office «Guidance on AI and data protection»: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

31 Ethics guidelines for trustworthy AI: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

32 Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/

- Where information about the AI entity's data processing activities can be obtained?
- How information about data processing is provided to individuals?
- Are data subjects informed about their rights?[33]

The Italian data protection authority mandated informing people about the use of their personal data in AI technologies through various means, including radio, television, newspapers and the internet. This decision pertained to the new ChatGPT technology and compelled the developer company, OpenAI, to implement a range of measures to ensure reliability, security and the protection of confidential information in the system.[34]

LACK OF BIAS AND NON-DISCRIMINATION

The issue of creating unbiased AI systems has been the subject of numerous discussions and studies in recent years. It is important to note that bias can be either inadvertently or intentionally introduced into a specific system. For instance, cases where credit or employment is denied to elderly individuals or single pregnant women. An infamous case involves Amazon halting the use of AI for personnel selection due to bias discovered in an algorithm that relied on word patterns in resumes, inaccurately processing information.

Therefore, AI systems should allow for human intervention. To adhere to the principle of non-discrimination, one needs to address: where and in what form human assessment and analysis are necessary? In which cases is fully automated decision-making acceptable?[35] If AI is used to analyse personal data, ensuring a critical approach to source selection, potential biases and assessing their impact on human rights is crucial. This is directly reflected in data protection legislation.[36] Therefore, implementing unbiased AI usage requires a comprehensive approach, analysing all stages of the system's lifecycle starting from the design phase.[37]

DATA MINIMISATION

The principle of data minimisation involves reducing the amount of information, especially containing personal data, to the minimum necessary level. Only the data required to achieve the processing objectives should be collected.[38] To ascertain compliance with this principle, one can consider questions such as:

- Are data collected solely for specific purposes (without excessive data)?
- Is there an analysis of the data volume?
- Is there a procedure for removing surplus data?

For instance, when forming a database (phone numbers, emails, etc.) for organising a training course, automatic material distribution and result assessment, there is no need to additionally collect residential addresses. If such information is collected, it needs justification. In other words, the principle discourages gathering data solely on the assumption that they might be useful in the future.

In the context of AI systems, challenges arise concerning the principle of data minimisation, as technologies often require significant data volumes. Among potential approaches to comply with this principle in AI systems, particular attention should be given to data processing planning.

33 Generative AI: eight questions that developers and users need to ask: https://ico.org.uk/about-the-ico/media-centre/blog-generative-ai-eight-questions-that-developers-and-users-need-to-ask/

34 Chat GPT : Garante privacy, limitazione provvisoria sospesa se OpenAI adotterà le misure richieste. L'Autorità ha dato tempo alla società fino al 30 aprile per mettersi in regola: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9874751#english

35 Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/

36 Article 5 of the GDPR.

37 Information Commissioner's Office "Guidance on AI and data protection": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

38 Article 9 of the GDPR.

Legal and technical experts should collaboratively determine appropriate data volumes, considering the specific context of their future use. AI systems can achieve greater statistical accuracy using various information sources. However, this approach can simultaneously increase the risk of privacy breaches. Hence, finding a balance between these aspects is crucial.

4. SAFE AND RELIABLE ARTIFICIAL INTELLIGENCE TECHNOLOGIES

In previous sections, the impact of advanced AI technologies on human rights and international principles, approaches, and methods for their legal regulation have been discussed. Next, the focus will shift to important measures regarding the management of intelligent systems. In other words, explanations will be provided on the necessary decisions to ensure AI technologies are safe and comply with legal requirements.

4.1. PRELIMINARY CONSULTATIONS AND TESTING

When it comes to AI technologies significantly impacting human rights, it is advisable to conduct prior consultations during the development, deployment, implementation, or procurement stages. These consultations should involve experts from various human rights spheres, especially regarding confidentiality matters.

Certainly, there might be concerns about commercial confidentiality in the private sector or state secrets restricting access to information for the general public. However, this should not imply that a particular technology is developed, implemented, and then society has to deal with the consequences. Developers or implementers of AI should initially guarantee that their innovations are safe for society. In case of negative incidents, they should demonstrate that they obtained sufficient external expert opinions to proceed with such a project.

Testing AI systems primarily helps identify risks related to human rights violations, such as discrimination or privacy breaches. During system analysis throughout testing, problems can be identified and measures can be taken to address them even before implementation.

4.2. SYSTEMATIC MONITORING AND ADAPTATION

After implementing AI, it is crucial to conduct systematic monitoring to identify issues that may arise in real operating conditions, particularly those risks not identified during testing. Monitoring should involve continuous damage assessment, system updates, or retraining machine learning models as needed. It should consider the performance of both technical system components (algorithms, hardware components, input data, etc.) and human operators involved in system operations.

For instance, a developer company introduced an AI-based facial recognition project in video surveillance systems. During testing, the system exhibited great results, accurately recognising faces in 99% of cases. However, after deploying this technology in a real environment, certain errors surfaced under specific conditions like poorly-lit faces or unusual viewing angles. Despite high accuracy in test data, the system might be less effective in real conditions due to differences not encountered during model training.

4.3. ANALYSIS OF STATISTICAL ACCURACY AND RELEVANCE OF DATA

Statistical accuracy is among the considerations that an AI system deems correct or incorrect. It is important to note that the term "accuracy" holds different meanings with regard to personal data protection. Accuracy, within data protection legislation, is defined as a fundamental principle requiring a guarantee that the personal data are accurate and, when necessary, kept up to date. It requires taking all reasonable measures to ensure that processed personal data are not "inaccurate or misleading about any fact" and, if necessary, are corrected or erased.

In the broad sense, accuracy in AI (and generally in statistical modelling) concerns how often the AI system predicts the correct answer, measured based on correctly labelled test data. Test data are typically separated from training data before training or are sourced separately. It is crucial to note that in many cases, the answers provided by an AI system are considered personal data. Therefore, in this document, "accuracy" is understood in the context of data protection law, while "statistical accuracy" pertains to the accuracy of the AI system itself.

Enhancing the statistical accuracy of AI system outputs is an important requirement to ensure adherence to the principle of fairness. However, this does not mean that the AI system must be entirely statistically accurate to comply with the principle of accuracy. In many cases, AI system outputs are not intended to be regarded as factual information about an individual. Instead, they represent statistically justified assumptions about what might be true about an individual now or in the future. To prevent misinterpretation of such personal data as factual, it is essential to ensure that records (or internal documents) indicate that they are statistically justified assumptions rather than unreliable facts. Records should include information on data origins and the AI system used to generate the result. If a conclusion was based on inaccurate data or if the AI system used to create it has a statistical flaw, this can impact the quality of the result.[39]

Data protection legislation, such as the GDPR,[40] defines statistical accuracy concerning profiling and automated decision-making. Organisations must apply "appropriate mathematical and statistical procedures" for profiling individuals as part of their technical measures and ensure the correction of any factors that might lead to inaccuracies in personal data to minimise the risk of errors. If AI systems are used to draw conclusions about individuals, it is necessary to ensure that the system has sufficient statistical accuracy for such purposes.

Overall, statistical accuracy as a measure depends on the ability to compare the system's conclusions to some "ground truth". For instance, a medical diagnostic tool detecting specific illnesses can make an assessment using quality test data containing known patient outcomes. In other fields, achieving ground truth might be unattainable because of a lack of quality test data or subjective judgments (for instance, which specific social media post is offensive, etc.).

Misunderstanding statistical accuracy may lead AI to be perceived as extremely accurate, while in reality, it merely reflects average estimates from a set of human labels rather than an objective truth. To avoid this, it is crucial to note that AI conclusions should not be regarded as absolute truth. Even if a system demonstrates high statistical accuracy with existing data, it does not guarantee similar effectiveness if certain group characteristics change or when applied to a different group in the future. AI performance can vary due to multiple factors and may become less statistically accurate over time.

Therefore, it is necessary to regularly evaluate such "biases" and retrain the model on new data if needed. Avoiding "contamination" of the system with outdated, inaccurate or erroneous data is crucial as this can distort or worsen outcomes.[41]

39 Under specification Presents Challenges for Credibility in Modern Machine Learning: https://arxiv.org/pdf/2011.03395.pdf.

40 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance): https://eur-lex.europa.eu/eli/reg/2016/679/oj

41 Information Commissioner's Office "Guidance on AI and data protection": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

4.4. DATA SEARCH AND QUALITY ASSURANCE

It is important to pay attention to the sources of data used for training AI models and consider several factors, including accuracy, representativeness and legality. In this context, the following questions need to be addressed:

- What data sources are used for training AI models?
- How and from whom were the data obtained?
- What proportion of the data was obtained from publicly available sources for AI training?
- On what legal basis is the data collection and processing conducted?
- How is the content of the original data assessed—manually or automatically?
- Are the original data representative, unbiased, and protected against unauthorised use?

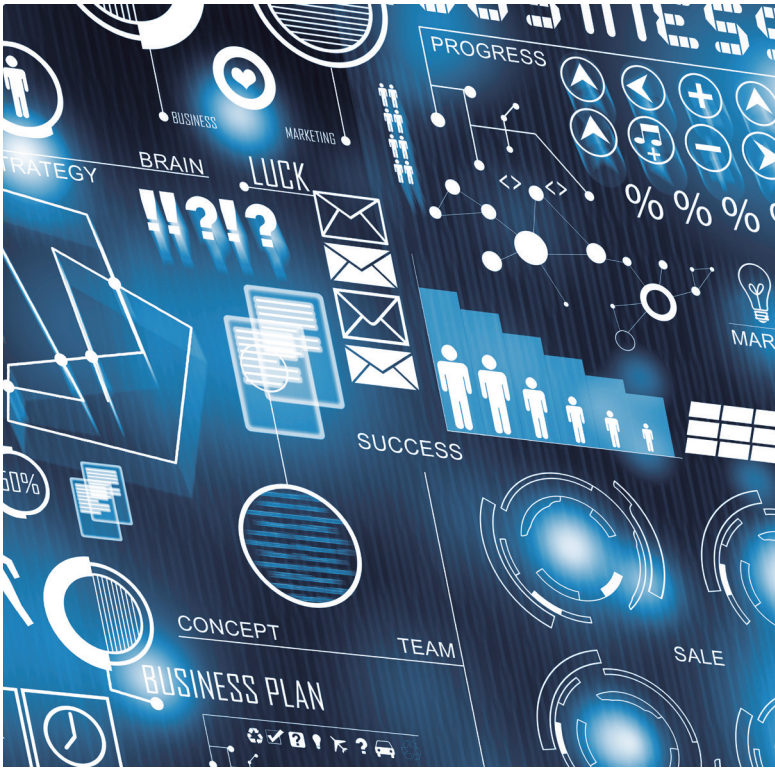
For example, the Singapore Personal Data Protection Commission additionally recommends considering certain issues for a better understanding of the quality of the training dataset to enhance the accuracy and productivity of AI models, specifically:

- Do the original data contain copyrighted information?
- Do the original data contain personal information?[42]

One of the risks in developing and using AI is the risk of bias, which can be caused by the algorithm's initial configuration and the quality of the collected data. To minimise this, the data used should be verified and accurate. Therefore, it is recommended to:

- Keep records of data origins.
- Conduct audits of datasets used in algorithm creation.
- Assess the quality of datasets used for system training.
- Regularly update the data used for system training.

Have separate datasets for training, testing and decision-making validation processes. Simultaneously, if possible, employ anonymisation tools. This means determining whether it is necessary for the data used to be associated with a specific person. If unnecessary, it is better to use anonymised information where individuals cannot be identified. This will help reduce the risks associated with processing and protecting personal data in AI projects and processes.[43]



42 Proposed advisory guidelines on use of personal data in AI recommendation and decision systems, 2023: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/legislation-and-guidelines/public-consult-on-proposed-ag-on-use-of-pd-in-ai-recommendation-and-systems-2023-07-18-draft-advisory-guidelines.pdf

43 General Recommendations for the Processing of Personal Data in Artificial Intelligence. Document approved by the Member Entities of the Ibero-American Data Protection Network in the 21 June 2019 session in Naucalpan de Juárez, Mexico.

4.5. RESPONSIBILITY SYSTEM

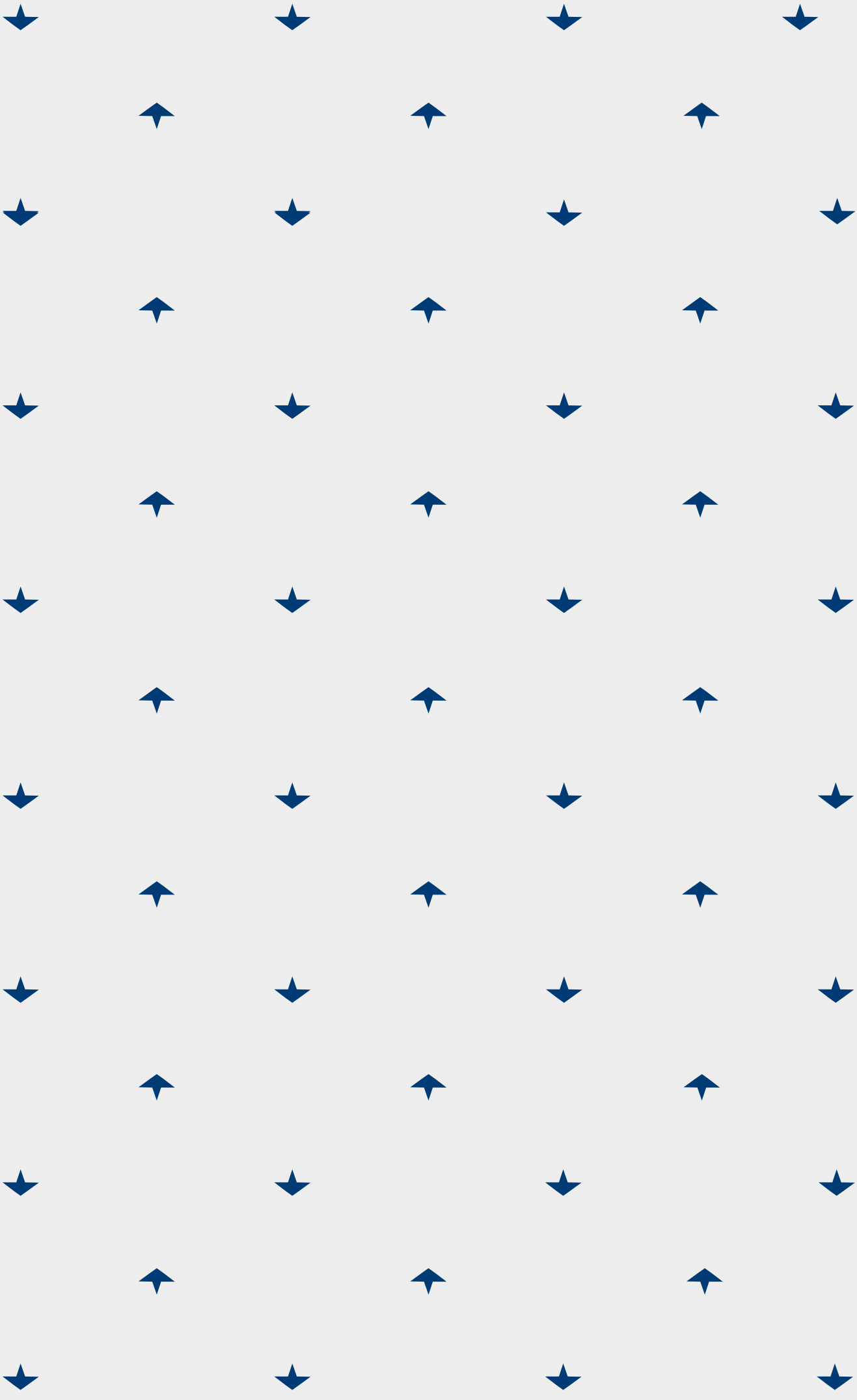
If errors occur in an automated system, it can lead to compromise, loss or incorrect handling of information. Therefore, it is important to have a clear system of responsibility for individuals developing, implementing or using AI systems. Currently, in Ukraine, there are no direct provisions in legislation requiring accountability from parties responsible for developing or using AI, nor mechanisms for controlling such systems. However, international best practices should be considered, as legislative regulation can protect the interests of citizens, businesses and the state by ensuring that AI system technologies are used ethically, transparently and responsibly.

Among the prevalent examples in the context of ethical and responsible AI use arises the question: who bears responsibility if an autonomous vehicle is involved in an accident that causes harm to a pedestrian? Is it the vehicle manufacturer, the software enabling decision-making, the sensor designer responsible for environmental perception, or the governmental authority permitting such a vehicle on roads? The issue of responsibility when AI operates autonomously is highly debated among legal experts. Some argue that if the event was caused by design flaws, the responsibility lies with the manufacturer. If it was a software glitch, then it lies with the developer. If it was programmed from the outset, then it lies with those who trained or deployed it, and so on. Some believe that all the mentioned entities share responsibility simultaneously. In any case, there must be a legal basis to address this issue and developed approaches depending on the level of risk and other characteristics of the machine. The same applies to systems operating based on personal data and making decisions that impact human rights.

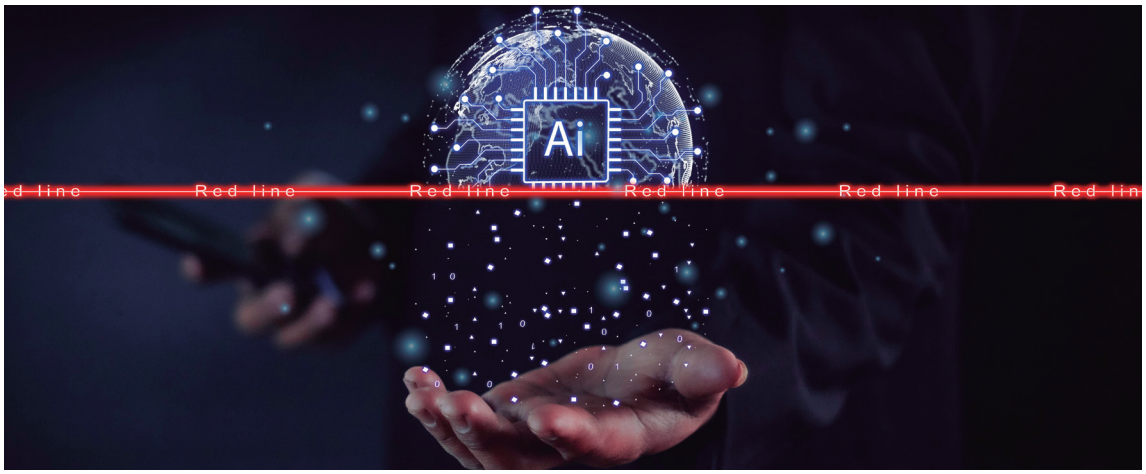
In this regard, it is important to consider jurisdictional issues, meaning the determination of powers and competencies of judicial or supervisory bodies in handling cases related to AI. This includes defining the subjects of jurisdiction, such as developers, suppliers, users of systems and so forth. The scope of application involves types of activities or situations. Given the transnational nature of modern technologies, it is also crucial to determine which legislative provisions apply when considering cases with international aspects or impacts.

Therefore, when it comes to the security and reliability of AI systems, it is necessary to have answers to questions like: what happens in the case of an unforeseen scenario? Reliability and security encompass a complex of 'what if' questions. Reliability scenarios and mechanism responses should be fully drawn up and anticipated. It is also important to understand how a human could intervene in the system if needed. The reliability of an AI system must be demonstrated throughout its lifecycle through audits.[44]

44 Blueprint for an AI Bill of Rights: A Vision for Protecting Our Civil Rights in the Algorithmic Age: https://www.whitehouse.gov/ostp/news-updates/2022/10/04/blueprint-for-an-ai-bill-of-rightsa-vision-for-protecting-our-civil-rights-in-the-algorithmic-age/



5. ENSURING THE PROTECTION OF PERSONAL DATA



As mentioned earlier, most modern AI technologies involve the processing of personal data. This means that one of the significant risks involves violating an individual's right to privacy. Unlawful or erroneous handling of confidential information about a person within AI systems can lead to negative consequences for that individual.

Therefore, stakeholders, including organisations or individuals developing, deploying or using AI, should ensure the protection of personal data throughout the entire lifecycle of the system. Specifically, maintaining a fair balance between the interests for which the intelligent system was created and the rights and freedoms of the individuals whose data this system affects.

5.1. DESIGNING A PERSONAL DATA PROTECTION SYSTEM

All entities processing personal data must design an appropriate system for their protection—privacy by design and privacy by default. The terms 'privacy by design'[45] and 'privacy by default'[46] were coined by the Information and Privacy

45 Privacy by design means that a person who collects data is obliged to build a system of data protection into all processes of its activities at an early stage of their design and must maintain such a system continuously in the future. In essence, the law focuses on the prevention of all possible risks, such as data leakage.

46 Privacy by default means that individuals whose data are processed do not need to take any action to protect their privacy, as this should be provided by default. That is, organisations should implement appropriate technical and organisational information security measures. The principle of data minimisation is relevant here: the less data an organisation collects and processes, the lower the risk of breaching the law.

Commissioner of Ontario, Ann Cavoukian.[47] In 2009, she published a document explaining that 'embedded privacy' means companies must actively consider data protection throughout the entire data processing lifecycle: from information collection to its deletion. This process should begin during the design phase, ensuring that all data are securely stored and then destroyed in a timely manner. The principles of privacy by design and privacy by default have been adopted as a standard in data protection by most countries. For example, Article 25 of the GDPR states:

> *'Considering the state of the art, the cost of implementation, the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, designed to effectively implement data protection principles, such as data minimisation, and integrate necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall apply appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility.'*

For instance, generative AI in the form of chatbots offers the ability to quickly and easily create various types of content. Well-known large language models (LLMs) include ChatGPT, Luminous or Bard. In many institutions, such tools have become part of the daily workflow, yet their usage is often unregulated. The fact that language models typically operate in the cloud carries various risks related to the breach of personal data protection. Therefore, the Commissioner for Data Protection and Freedom of Information in Hamburg published a checklist in November 2023 regarding the use of chatbots based on large language models (LLMs) in compliance with personal data protection laws. This document highlights key aspects to consider when using LLM-based chatbots, including:

> *"Considering the current level of development, implementation costs, specifics, scope, context, and purposes of processing, as well as the varying likelihood and severity risks to the rights and freedoms of individuals resulting from the processing, the controller must, at the time of determining the processing means and during the actual processing, implement necessary technical and organisational measures, such as using pseudonyms, designed for the effective realisation of data protection principles, including data minimisation, and include necessary guarantees in processing to comply with the requirements of this Regulation and ensure the protection of data subjects' rights. The controller must employ appropriate technical and organisational measures to ensure that, by default, only those personal data necessary for each specific purpose of processing are processed. This obligation applies to the amount of collected personal data, the extent of their processing, the period of their storage and their accessibility."*

For instance, generative AI in the form of chatbots offers the ability to quickly and easily create various types of content. Well-known large language models (LLMs) include ChatGPT, Luminous or Bard. In many institutions, such tools have become part of the daily work process, but their usage is often unregulated. The fact that language models typically operate in the cloud carries various risks related to the breach of personal data protection. Therefore, the Commissioner for Data Protection and Freedom of Information in Hamburg published a checklist in November 2023 regarding the use of chatbots based on large language models (LLMs) in compliance with personal data protection laws.[48] This document

47 Ann Cavoukian, Ph.D. Privacy by Design. The 7 Foundational Principles: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

48 Checklist for the use of LLM-based chatbots: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checklist_LLM_Chatbots_EN.pdf

highlights key aspects to consider when using LLM-based chatbots, including:

- Formulating clear internal guidelines on when and under what conditions to use generative AI tools.
- Involving a Data Protection Officer (DPO) in developing internal instructions, organising appropriate processes for assessing data protection impact (DPIA).
- Ensuring data confidentiality in the results of AI work.
- Eliminating risks related to data leaks, bias and discrimination in AI work results, etc.

Therefore, legislation, and in particular the GDPR, mandates ensuring an individual's right to protect personal data at every stage of their processing, starting from the design of the AI product or service. The 'privacy by design' approach is used more for risk prevention rather than consequence elimination. In other words, people should not have to assert their right to privacy; it should be protected by default.[49]

5.2. RISK ASSESSMENT

Risk assessment is an essential component of designing a system for protecting personal data and information processing using AI. This pertains to both the technical protection of systems and the essence of their function (clarification: for what purposes AI is used), as well as compliance with data protection laws. According to international provisions,[50] individuals or entities processing personal data should conduct risk assessments to anticipate situations that could threaten the rights and freedoms of individuals even before they occur. This process can take various forms and apply to both the technical aspect of system operation (see Section 4) and organisational processes. For example, in European legislation, Data Protection Impact Assessment (DPIA) is a procedure outlined in Article 35 of the GDPR and other documents defining international data security standards. DPIA is a process intended to help analyse, identify and minimise risks to personal data during their processing.[51] Failure to conduct a required DPIA may lead to accountability. For instance, Article 84 of the GDPR specifies that '... the controller shall be responsible for conducting an assessment of the impact of the envisaged processing operations on data protection to determine, in particular, the origin, nature, likelihood, and severity of such a risk.

The outcome of the assessment should be taken into account when determining the appropriate measures needed to ensure that the processing of personal data complies with this Regulation.'

In other words, the legislator emphasises that DPIA is a systematic process that should be integrated on an ongoing basis. That is, every institution or organisation should develop its methodology considering the specifics of its activities' and

49 The manual «Risk analysis when processing personal data: what is important to know?». For more information on the risk assessment methodology, please follow the link: https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf

50 Standards ISO-29134 "Guidelines for privacy impact assessment", ISO-31000 "Risk management. Principles and guidelines", ISO-31010 "Risk management. Risk assessment techniques".

51 "The Practical Guide for Data Protection Impact Assessments subject to the GDPR" published by the AEPD. Standards ISO-29134 "Guidelines for privacy impact assessment", ISO-31000 "Risk management. Principles and guidelines" and ISO-31010 "Risk management. Risk assessment techniques".

the need for risk assessment. Overall, the main goal of this process is to answer questions like:

- What threats exist?
- What are their sources?
- What consequences could arise?
- What needs to be done to mitigate them?

Assessment should be conducted when launching a new project, setting new goals, collecting a different type of data, especially those belonging to special categories, changing the software used for data processing, etc. Additionally, it is advisable to conduct assessments in the following situations:

- Merging multiple databases into one (not recommended as this may pose numerous threats).
- Creating new databases or implementing new information processing procedures.
- Involving new parties. For example, executing projects using third-party suppliers.
- Adding new features to an existing product or service.

In the current Ukrainian legislation, there are no obligations regarding the types of processing subject to assessment. However, European standards, which Ukraine should align with, include the following list. For instance, Article 35(3) of the GDPR defines three types of processing that always require DPIA:

Systematic and extensive profiling of individuals: (A) 'Systematic and extensive evaluation of personal aspects relating to individuals based on automated processing, including profiling, and on which decisions have legal effects concerning the individual or similarly significantly affect the individual.'

Large-scale processing of special categories of data: (B) 'Large-scale processing of special categories of data referred to in Article 9(1), and personal data on criminal convictions and offences referred to in Article 10.' Public surveillance: (C) 'Systematic and extensive monitoring of a publicly accessible area.' According to Article 29 of the GDPR, the data collector establishes appropriate instructions for their processing and protection. The EU Working Group on Data Protection published[52] guiding principles that may serve as indicators of high-risk processing, such as:

- Processing personal data using innovative technologies, particularly AI.
- Applying automated decision-making.
- Processing medical, biometric or genetic data (except when performed by healthcare professionals to provide assistance to an individual).
- Processing involving tracking an individual's geolocation or behaviour, including online environments.
- Processing a child's personal data, especially for marketing purposes.
- If the data processing poses a threat to the health or physical safety of individuals.
- Employing extensive profiling of individuals.

According to the Digital Services Act (DSA), which came into effect in the EU in 2022, special provisions are outlined for large online platforms or search engines—Very Large Online Platforms (VLOP) and Very Large Search Engines (VLSE), with over 45 million users. These entities are obliged to conduct a comprehensive risk assessment annually regarding the potential adverse impact of their services, such as access to illegal goods, content, or the spread of disinformation. Additionally, VLOP and VLSE must conduct a comprehensive analysis of threats to fundamental human and citizen rights. For instance, in response to this, Google announced a series of changes to its policies. Specifically, regulators have been granted expanded access to data related to targeted advertising campaigns, and more information regarding service moderation and search engines has been disclosed. Meta reported that Facebook and Instagram have ceased running advertising campaigns targeted at teenagers.

However, analysing the recommendations of state regulators in the field of personal data protection in European countries, most emphasise that even if data processing using AI systems does not fall into high-risk categories where the law requires conducting DPIA, considering technological advancements and the lack of a

52 Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01): https://ec.europa.eu/newsroom/article29/items/611236

definitive understanding of the real impact on human rights and freedoms, conducting risk assessments is still advisable.[53]

The risk assessment process can occur in several stages. For instance, initially by analysing the directions of work in the field of personal data processing overall. Then, by identifying the purpose for conducting this procedure since the analysis scenario and its methodology content will depend on the analysis objective, as well as the required time, resources, and expected outcome. To begin, a risk assessment methodology focused specifically on this activity should be developed. When there is a detailed subject profile (specifically an organisation), a defined objective and analysis methodology, the risk assessment stage follows.[54] Because AI usage projects vary significantly, including different objectives and processes of personal data processing, an individual adapted risk assessment methodology should be developed, broken down into stages for technology application. Third-party experts with appropriate qualifications in this field can be engaged to perform this process. Considering the complex and dynamic nature of AI, this not only helps effectively tackle data protection challenges but can also serve as a competitive advantage.

53 Information Commissioner's Office "Guidance on AI and data protection": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

54 The manual «Risk analysis when processing personal data: what is important to know?». For more information on the risk assessment methodology, please follow the link: https://decentralization.gov.ua/uploads/library/file/774/Posibnyk_ocinka-ryzykiv-ZPD.pdf

5.3. DETERMINING THE GROUNDS FOR PROCESSING PERSONAL DATA

If the information system involves the processing of personal data, such activity must be justified by law. That is, there must be a legal basis. Article 11 of the Ukrainian Law 'On Personal Data Protection' defines the grounds for processing personal data:

- Consent of the personal data subject to the processing of their personal data;
- Permission for the processing of personal data granted to the data controller in accordance with the law exclusively to perform their duties;
- Conclusion and execution of a legal act to which the personal data subject is a party or which is concluded for the benefit of the personal data subject, or to take measures preceding the conclusion of the legal act at the request of the personal data subject;
- Protection of vital interests of the personal data subject;
- Necessity to fulfil the obligations of the data controller prescribed by law;

- Necessity to protect the legitimate interests of the data controller or a third party to whom the personal data are transferred, except when the needs of protecting the fundamental rights and freedoms of the personal data subject in connection with the processing of their data outweigh such interests.

Although the use of information systems does not fundamentally differ from other forms of data processing, there are still some peculiarities. For example, systems based on machine learning require the use of data for training before they are applied in the operational phase of the AI system. Given that this training phase is significantly different from the operational implementation stage of the AI system. its sole purpose is to enhance the productivity of the AI system. At the same time, it is important to note that the legal basis of 'scientific research' itself cannot be a legal basis for processing, only those legal grounds explicitly listed in the law.[55]

It is important to note that if AI systems are deployed by a subject vested with authority, then according to Article 19 of the Constitution of Ukraine, its officials must act solely on the basis of the Constitution and laws of Ukraine, within the limits of authority, and in the manner provided for therein. In view of this provision, for example, bodies of state power or local authorities may process personal data (any action or set of actions) only in the presence of powers, a legal basis, a justified purpose, and in a manner provided by law. That is to say, it is not necessary to obtain the consent of the personal data subject in those cases when permission to collect information is directly provided by law. At the same time, it is not enough to have authority; there must be a justified purpose and a clear procedure.

In European legislation, the legal bases for processing personal data are outlined in Article 6 of the GDPR:

55 National Commission for Information Technology and Civil Liberties of France (CNIL). Access mode: https://www.cnil.fr/fr/intelligence-artificielle/ia-comment-etre-en-conformite-avec-le-rgpd

1. The data subject has given consent to the processing of their personal data for one or more specific purposes.
2. Processing is necessary for the performance of a contract to which the data subject is a party or for steps taken at the request of the data subject prior to entering into a contract.
3. Processing is necessary for compliance with a legal obligation to which the data controller is subject.
4. Processing is necessary to protect the vital interests of the data subject or another natural person.
5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
6. Processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, particularly if the data subject is a child.

Determining when a lawful basis applies depends on the specific purposes and context of the processing. Often, several grounds are applied, depending on the particular case of data processing. None of the listed bases can be considered superior to or more important than the others. Before implementing technologies based on personal data, it is advisable to consider the so-called three-step test, in which it is necessary to:

- Identify the legal basis.
- Ensure that the processing is necessary to achieve a specific purpose.
- Balance it with the interests, rights and freedoms of the individual.[56]

56 Information Commissioner's Office "Guidance on AI and data protection": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

5.4. DEFINING THE PURPOSES FOR PROCESSING PERSONAL DATA

An AI system which is based on the use of personal data should always be developed, trained and deployed with a clearly defined purpose (goals). It needs to be established prior to the development of a project (product or service). A clear understanding of why specific information is processed is necessary to implement the principle of "purpose limitation" and ensure fairness, legality and transparency in personal data processing, including determining the necessary level of their protection.

According to the "purpose limitation" principle, it is necessary beforehand to define, justify and document the real reasons and purpose for said data collection, as this will prevent their use for unlawful purposes. For example, before installing surveillance systems with AI technologies, it is essential to define their purpose and ensure their legality. Additionally, it must be established that achieving this purpose is not possible by other means that involve less intrusion into privacy. Vague or general descriptions such as "for improved performance of tasks" are insufficient. Furthermore, it is crucial to ensure that personal data will not be used for unforeseen purposes or unlawfully transferred to third parties without authorised access.

Personal data may be processed to achieve specific real purposes, and these purposes should be as specific as possible, achievable and outlined in internal documents (policies) regulating work in this field. The use of data to fulfil additional or new tasks is possible if:

1. The new purpose of processing personal data is compatible with the primary purpose.

In such a case, a new legal basis for working with the data is not required, but assessing whether the updated purpose is truly compatible with the initial one must be objective. To do this, it is necessary to consider the following factors:

- How closely the primary purpose is related to the new one.
- The context in which the personal data were initially processed.

- The specificity and nature of the data (for instance, whether they belong to a special category, etc.).
- The likelihood of negative consequences for individuals whose data are being processed.
- The ability to ensure an adequate level of protection for processing the new information.

For example, implementing an AI-based AI system occurs in stages. Initially, there is training involving the design and development of the AI system. Then, there is the operational deployment of the AI system obtained in the first stage. From the perspective of personal data protection, these two steps do not align with the same goal and hence should be separated. In both cases, the purposes of processing personal data should be separately defined, clear and have legal grounds.[57] For instance, facial recognition systems can be used for various purposes, such as crime prevention or authentication and tagging individuals on social networks. Each of these applications may require a different legal basis.

2. A legal norm has emerged that requires or allows data processing for a new purpose.

For example, due to corresponding changes in legislation, the authority's powers have increased, granting it the right to perform additional functions related to processing personal data.

5.5. DEFINING THE ROLE DURING THE PROCESSING OF PERSONAL DATA

Understanding the role of stakeholders in AI data processing is necessary in order to define the extent of their rights and obligations. For instance, based on international practice, significant attention is placed on decisions to be made by the data controller. This includes:

- The source and nature of the data used to train AI models.
- The intended outcome of the model (predictions or classifications).
- General types of machine learning algorithms to be used for model creation (e.g., neural networks).
- Selection of features for use in each model.
- Key model parameters (e.g. complexity of decision trees, number of models in the lifecycle).
- Testing and updating methodologies for the models.[58]

When AI systems involve multiple organisations in data processing, determining roles can be challenging. Questions may arise regarding scenarios where an organisation becomes the data controller. For example, an organisation provides cloud storage services and a set of machine learning tools. Users of this service, by law, might be considered data controllers as they decide which data and models to use, the parameters of the model and the processes for evaluation, testing, and updates. However, the service provider might be the data processor, as it primarily handles technical aspects, storage configurations and cloud architecture.

Another scenario involves a supplier (data processor) offering a resume screening tool for candidate assessment, starting to request a substantial amount of information from the data controller about each candidate. If the data controller purchases this system, it is essential to evaluate whether collecting such volumes of personal

57 The same position was officially published by the French National Commission for Information Technology and Civil Liberties (CNIL). Access mode: https://www.cnil.fr/fr/intelligence-artificielle/ia-comment-etre-en-conformite-avec-le-rgpd.

58 Information Commissioner's Office "Guidance on AI and data protection": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

data from candidates is justified. If not, it is necessary to ask the supplier to modify the system or seek alternatives.

These examples highlight the complexity of determining roles, especially when multiple AI subjects are involved. It underscores the need for a clear understanding of responsibility within data protection laws and additional research on practical instances.

5.6. ENSURING THE RIGHTS OF PERSONAL DATA SUBJECTS

Designing a personal data protection system within AI technologies requires a clear understanding and adherence to an individual's informational rights. According to the law, every individual possesses non-property rights to their personal data. These include:

1. Knowing the sources of data collection, the purpose of data processing, and the location of the data owner or processor. Individuals can authorise designated individuals to obtain this information, except in cases specified by law.
2. Receiving information about the conditions for granting access to personal data, including details about third parties receiving their personal data.
3. Access to their personal data.
4. Receiving a response, no later than thirty calendar days from the date of the request, regarding whether their personal data are

being processed and obtaining the content of such data, except in cases specified by law.
5. Objecting to the processing of their personal data by presenting a substantiated request to the data owner.
6. Requesting the modification or deletion of their personal data by any data owner or processor if the data are processed unlawfully or are inaccurate.
7. Protection of personal data from unlawful processing, accidental loss, destruction, damage caused by intentional concealment, non-provision or untimely provision, as well as protection from the dissemination of false or misleading information affecting the individual's honour, dignity and business reputation.
8. Filing complaints regarding the processing of their personal data to the authorised body or court.
9. Implementing legal means of protection in case of violations of personal data protection laws.
10. Imposing restrictions on the right to process their personal data while giving consent.
11. Withdrawing consent for the processing of personal data.
12. Understanding the mechanism of automated personal data processing.
13. Protection from automated decisions that have legal consequences.[59]

Below we delve into some of them in more detail.

RIGHT TO INFORMATION AND DATA ACCESS

This right enables an individual to inquire about:

- Whether their personal data are being processed by the owner or processor of the data (data controller or data processor).
- What specific data are being processed (categories and types).
- The legal basis and purpose for the processing.[60]

Questions may also pertain to other technical and organisational data processing processes: internal policies, security systems, data retention periods, disclosures, third-party transfers, etc. If an individual's data are not processed, it is necessary to notify them of this fact (ignoring a request is not acceptable). If the data are processed, confirmation of the fact is required. If an individual wishes to access their data, this request should generally be fulfilled, except in cases defined by law. The Ukrainian Law "On Personal Data Protection" not only guarantees the right to access personal data but also establishes principles such as cost-free access (Article 19 of the Law) and promptness (Article 17 of the Law). Therefore, every individual should have the opportunity to review their information freely, without any charge. This might raise questions about the volume of data, which should always be clarified.

It is important to note that such a request might be perceived as a description of data, i.e., what information is being collected. According to the law, specifically, personal data should be provided. If these were filled-out forms, for example, to obtain a store discount card, it refers to those specific data. If fulfilling the request is overly complex, the individual should be informed, citing reasons for the inability to comply with the request and presenting any alternative options. Thus, it is crucial to adhere to the concept of privacy-by-design during the model development stage. This way, information privacy specialists can foresee the legislative aspect of ensuring an individual's right to information and access to their data, except in cases defined by law. This includes developing policies and other internal instructions to facilitate an individual's access to information about:

- purposes of processing;
- types and categories of personal data;
- about the recipients or categories of recipients to whom the data have been or will be disclosed;
- the period of data retention or the criteria for determining this period;
- the rights of the person, in particular to rectify or delete their data, or to restrict or object to their processing;
- the right to lodge a complaint with a supervisory authority;

59 Article 8 of the Ukrainian Law "On Personal Data Protection".

60 The right of access of a personal data subject is enshrined in Article 15 of the GDPR.

- the source of the personal data, if they were not obtained from the data subject;
- availability of an automated decision-making process, including at what stage of data processing this is applied;
- conditions and means of data transfer protection if personal data are transferred to a third country or international organisation.[61]

RIGHT TO ERASURE

The right to erasure, also known as the "right to be forgotten", grants individuals the ability to request the deletion of their personal data. According to Article 8 of the Ukrainian Law "On Personal Data Protection", an individual has the right to present a substantiated request to object to the processing of their personal data and to demand their deletion if the data are processed unlawfully or are inaccurate. According to Article 17 of the GDPR, individuals have the right to request the deletion of their personal data if, among other reasons, the data are no longer necessary for the purposes for which they were collected, the subject withdraws their consent for data processing, or the data are processed unlawfully, except in cases defined by law.

In AI systems that utilise personal data for training and operation, ensuring the right to erasure requires implementing technical and organisational measures. These measures should ensure the capability to delete data upon request by an individual and fulfil this request within a reasonable timeframe. It is crucial to ensure that the deletion does not disrupt the objectives and functions of AI systems, which may include pattern recognition, model training or other tasks. Such procedures should consider the system's specific operations and the ability to delete or anonymise data from various sources and databases.[62]

RIGHT TO PROTECTION FROM AUTOMATED DECISION-MAKING

Any modern technology is prone to failure, errors, cyber-attacks and other issues that could have unforeseen consequences for individuals and society at large. According to national and international laws,[63] individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects, except in cases determined by law.

Legislation does not prohibit the use of AI for automated decision-making if these decisions have legal grounds and are carried out in a lawful manner. Certain guarantees for such processing must be established. This includes considering "specific circumstances and context" and implementing technical and organisational measures to ensure its "fairness and transparency". These measures should:

- Ensure the processing of personal data considers risks to the rights and interests of individuals (see section 5.2 Risk Assessment).
- Prevent discriminatory impacts based on specific categories of data.

There should also be the possibility to opt-out of automated systems where relevant. According to Article 8 of the Ukrainian Law "On Personal Data Protection" and Articles 13 (2)(f) and 14 (2)(g) of the GDPR, individuals whose data are processed should be informed about the use of automated systems, including providing "meaningful information about the logic involved in automated decision-making, as well as the potential consequences" of such processing for them. Timely human control and intervention should be ensured if the automated system malfunctions, produces errors, or at the data subject's request, etc.

There are many reasons why people may not want to use an automated system: it can lead to unpredictable results, reinforce biases or be inaccessible; it can simply be inconvenient or replace a paper or manual process to which they are accustomed. However, individuals often encounter a lack of alternatives. This is an incorrect approach to ensuring legal safeguards. A person should have the right to choose or object to the use of automated processing, except when such a system is established in accordance with legal

61 According to Article 46 of the GDPR.

62 Guidelines on Personal Data Processing Using Artificial Intelligence Technologies, FIIAPP.

63 Article 22 of the GDPR.

requirements, in the interests of national security or economic prosperity. In any case, measures should be taken to prevent adverse consequences for individuals.

In practice, questions may arise: what processing is considered automated? AI systems perform various roles, meaning they can participate in different stages of decision-making processes. When AI makes a decision that has legal consequences for individuals, the following questions should be considered:

- What type of decision is it (is it solely automated)?
- When is this decision made?
- In what context does the system make the decision?
- What steps lead to this decision?

As mentioned earlier, legislation requires ensuring security measures during the processing of personal data for conducting automated decisions that have legal or similarly significant impacts on individuals. These measures include the right of individuals to:

- Request human intervention.
- Express their point of view.
- Challenge decisions made about them.
- Receive an explanation of the logic behind the decision.

Human intervention should involve analysing the decision regardless of whether the processing is fully or partially automated.[64] Therefore, it is also necessary to:

- Consider the system requirements necessary to ensure meaningful human review from the design phase.
- Develop and provide appropriate professional training for individuals reviewing decisions.

It is essential to provide information on the specifics of automated decision-making, especially regarding the data sources used for its determination. For instance, if decision outcomes are

64 The Alan Turing Institute guidance on 'Explaining decisions made with Artificial Intelligence.

provided through a website, there should be a link or clear information allowing individuals to contact a staff member who can intervene without unnecessary delays or complications. All records of AI-generated decisions, information about whether an individual requested human intervention, expressed their views, challenged decisions, or whether the decision changed as a result, should be kept for a certain period.[65] Also, additional aspects need to be considered within complex AI systems:

- Automation bias. This refers to a situation where decision-makers trust the results generated by the system without applying their own judgment or questioning any potential errors in its conclusions. For instance, medical software could mix one patient's history with that of another, leading to denial of means of pain reduction, or an institution adopting an automated work evaluation system resulting in the dismissal of employees based on program-generated decisions without giving them the chance to appeal. Hence, human intervention for data verification is crucial.
- Lack of interpretability. Some types of AI may provide results that are challenging for humans to interpret, like those based on complex deep learning models. If AI results cannot be easily interpreted, and alternative explanations are insufficient or unreliable, there is a risk that individuals will not properly assess the results in their decision-making.

Therefore, understanding the aspects of risk associated with each option and ensuring clear areas of responsibility and effective risk management policies is crucial.[66]

65 Guidance on the documentation of the European Guidelines for Automated Decision Making and Profiling. Access mode: https://ec.europa.eu/newsroom/article29/items/612053.

66 Information Commissioner's Office "Guidance on AI and data protection": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

Омбудсман України
Ombudsman of Ukraine

Фінансується
Європейським Союзом

FIIAPP
COOPERACIÓN ESPAÑOLA

Ministry
of Digital Transformation
of Ukraine