# ISSUE OF PRIVACY IN AI ERA: AUTOMATED DECISION-MAKING AND REMOTE IDENTIFICATION

***Tokareva Vira***
*Candidate of Legal Science, Associate Professor of the Department of Civil Law, National University "Odessa Law Academy"*
*ORCID ID: 0000-0002-8409-1477*

**Abstract.** In order to attain human rights and participate in social and political life, it is necessary to be a part of the network and fully utilize the latest technologies. On the web, a natural person is transformed into a digital profile or digital identity that is represented by digital projection. Furthermore, the importance and significance of artificial intelligence programs, known as a "black box", which analyze the actions of subjects in the network, learn, and are nearly capable of making autonomous decisions, is on the rise.

The "black box" helps on making decisions with individual in the following matters: assessing credit approval, employment, pre-trial investigation decisions, preventive detention through remote biometric identification or wiretapping, and other similar matters. There is a concern about the consequences of potential delegating decision-making power to the automated system. Nowadays, the final decision is made by any subject, even if automated systems are involved in decision analysis. Such analyses are conducted using all available data collected in the network, including a person's profile (set of personal data). Moreover, modern biometric identification technologies, which can be used to identify not only the face, but also the manner of walking and movement, can be used to identify people by cameras.

Furthermore, the excessive aggregation and automated processing of personal data, violation of laws regarding cross-border data transfers from the EU to the USA, and frequent hacker attacks have resulted in concerns about privacy interference, surveillance, and wiretapping for every person in society. Edward Snowden and Julian Assange's public disclosure and prosecution, along with the scandals related to personal data manipulation in the United States and Brexit, are of public concern. In addition, the analysis of big data for the development of machine learning raises the issue of establishing legal guarantees for the protection of individual rights to privacy due to the lack of transparency in the use of automated decision-making systems and the application of such systems without human intervention.

The use of automated decision-making systems in the government and private sector is based on the aim of ensuring national security, which includes prevention, detection, investigation of crimes, predictive analysis of offenses, extend the quality of public services and other related matters. Commercial organizations use automated system technologies (transport organizations, banks, supermarkets, cafes) to ensure security, facilitate access to financial products and increase sales.

The latest technologies and human interconnections in a socio-technical network have resulted in a society becoming more interconnected and influenced by each other. The above evidence indicates that there are all the necessary factors to establish a dictatorship, just like the one described by J. Orwell and other dystopian authors.

All of the above testifies to the relevance of studying human rights problems in the context of making significant decisions with assistance of automated systems and the remote biometric identification, the constant aggregation and processing of personal data to ensure national security, the development of technologies, and the search for a balance between privacy and security in such circumstances.

**Keywords:** AI, human rights, personal non-property rights, Big Data, Internet of Things, biometric identification, remote identification, EU law, personal data.

**Research methods.** The study's methodology included a set of legal methods that were both general and specific, such as the dialectical method, formal-logical method, method of analysis and synthesis and comparative legal method. The dialectical method allowed for the study of the relationship and interdependence between processes of digital transformation and the development of legal regulation.

By using the formal-logical method, the definition of biometric data and identification could be investigated and considered in accordance with normative legal acts and judicial practice. The use of the formal-logical method helped to consider the problematic issues that arise from the use of the latest identification technologies, which include biometric identification. The use of remote biometric identification and video surveillance, which is almost universal, pose a threat to privacy. The challenge is to find a balance between interference in the private lives of individuals and ensuring national security (such as the need to prevent, solve, and investigate crimes, predictive analytics, the development of technologies and public services, etc.). In addition, the challenge is to balance interference in private life, data collection, and the advancement of modern technologies, such as artificial intelligence, Big Data, IoT and the latest cancer drugs, etc.

The method of analysis and synthesis played a significant role in the study, as it enabled to analyse the risks of automated decision-making systems, big data, and remote biometric identification to fulfil individuals' rights. The method was used to determine and explore the risks of system biases that pose a major danger to human rights posed by automated systems and Big Data. Analysing the consequences of the opaque functioning of algorithms and the impartiality of the system became possible with the application of the method. The opacity of algorithms means that when it's unclear the reason a certain decision of making by algorithms, people try to add logic to it, which is proposed to call "algorithmic or math washing".

By applying a comparative legal method, it is possible to analyze the similarities and differences between the legal approaches used by states when regulating the issues privacy and AI.

## 1. The significance and role of biometric identification.

Identification is crucial in the development of information and communication technologies. Traditional identification methods when subjects are at a distance from one another, do not meet the needs of the information society. Furthermore, there is no uniform terminology or hierarchy for identifying of subjects of legal relationships on the Internet.

The expansion of electronic payments has an impact on the development of payment system legislation and measures to combat illegalization (laundering) of proceeds from crime and terrorism. All these processes are interconnected in terms of implementing automated decision-making systems and identification.

The need to provide private companies and the state authorities with an instrument for safe identification of a natural person via the Internet is due to the significance of electronic identification for providing public and banking services electronically.

Online identification is distinct from physical identification because special subjects, known as information providers (intermediaries), own the technological infrastructure of identification and store and process data about individuals and their behavior. The provision of personal data subjects to providers results in relative identification conditions that determine the responsibility

of information providers (intermediaries) and their ability to disclose data about their own customers and users when requested by law enforcement agencies.

When data is disclosed about their own users to information providers, it results in absolute identification and the subject can be identified by both the identifying person and other individuals.

On the Internet, identification features of a person are identifiers or personal data that allow for identification of a natural person in a virtual space. Given their special status, they are subject to legal protection.

The conventional identification methods used today should include name, surname, date and place of birth, gender, citizenship, individual insurance, and tax numbers. In most countries of the world, these identifiers are referred to as traditional means of identification. However, the full identification of an individual cannot be guaranteed due to the repetition of traditional identifiers among individuals.

Biometric data is now being utilized in an active way, in addition to conventional identifier methods such as digital codes and non-literal ciphers. Up until the fall of 2001, biometric identification systems were mostly used by the military-defence sector and to a lesser extent the commercial sector. The development of biometric identification systems was triggered by the terrorist attacks on September 11, 2001 in the United States. Thus, the development of biometric identification systems is expected to occur in the United States and then spread to other countries. A subcommittee of JTC 1/Sc37 dedicated to biometrics was created within the International Organization for Standardization's framework to create uniform standards for the use of biometric data [1].

According to the Law of Ukraine "On the Unified State Demographic Register and documents confirming the citizenship of Ukraine, certify the person or his special status" biometric data is a collection of information about a person that is based on their characteristics and is sufficiently stable and distinguishable from similar parameters of others (such as digitized signatures, facial images, and fingerprints) [2].

S. Bryginets notes that the bias against widespread application of biometric identification, known as the "Mark of the Beast', has been a struggle in Ukraine until recently. [3]. However, the ultimate point in this matter is to reflect the Supreme Court's decision in the panel of judges of the Cassation Administrative Court of 26.03.2018. in case No. 806/3265/17 [4].

In accordance with paragraph 14 of Article 4 of EU Regulation 2016/679, biometric data is personal data that is acquired through specific technical processing that pertains to the physical, physiological, or behavioral traits of an individual and also confirms their identification, such as facial images or fingerprint data.

As stated in the Guide 3/2019 of the European Board for the Protection of Personal Data on the processing of personal data with the use of video devices that the data are considered biometric data within the meaning of EU Regulation 2016/679, the data must be the result of special technical processing and various measurements of physical, physiological or behavioral characteristics [5]. Therefore, a photo or video taken by an individual cannot be considered biometric data in accordance with Article 9 unless special technical processing is used to facilitate the unambiguous identification of that individual. Biometric data processing is essential for special categories of personal data, which uniquely identifies a natural person (Article 9). The analysis of Articles 4 and 9 of EU Regulation 2016/679 indicates that in order to process biometric personal data, following criteria must be taken into consideration: the nature of the data relating to the physical, physiological or behavioral characteristics of an individual; means and methods of processing, they must be obtained as a result of specific technical processing; processing data serves the

purpose of uniquely identifying an individual. According to the general rule under Article 9 of EU Regulation 2016/679, the processing of biometric data in order to uniquely identify an individual is prohibited.

Furthermore, the risks are highlighted due to the fact that biometric data stays unaltered in the majority of instances.

As biometric data cannot be adjusted in a manner that is proportionate to the risks for the individual. This circumstance can be directly or indirectly found in the definition of biometric personal data in document 4/2007 'On the concept of personal data' of the Data Protection Working Party) [6]. The document states that biometric data is characterized by biological properties, physiological characteristics, character traits, and behaviour that is distinctive to a particular subject and can be empirically observed, despite the probability of indicators being measured. Examples can include: fingerprints, retina, facial structure, voice, hand geometry, vein pattern, and behavioural characteristics such as signatures, keystroke styles, gaits, speech styles, and more. It is crucial to emphasize that biometric data on one hand represent information about a particular natural person and, on the other hand, the characteristics of the existing association between the pertinent information and that individual.

In accordance with the UK Personal Data Protection Act of 2018 biometric data is personal information that is obtained through special technical processing that involves the physical, physiological, or behavioural characteristics of a person and allows or confirms their unique identification. For instance, facial images or fingerprint data (section 205) [7]. The significance of biometric data lies in its capability to identify individuals uniquely and distinguish them from other types of data. With the use of biometric data, government agencies can accurately determine a natural person's location and activities.

Edward Bridge v. The Chief Constable of South Wales Police provides a detailed analysis of the function of biometric automatic face recognition technology [8]. According to the Court of Appeal, the ability of automatic facial recognition technology to distinguish between two images is based on analyzing biometric data (such as measurements or facial features) taken from a digital photo of the face and comparing it to biometric facial data from images stored in the database. As explained by the Court, this technology enables to capture a face image of every person passing by CCTV cameras installed in police vehicles or on poles on public roads. Similarly, the Court asserted that these cameras allow to captured and processing of digital images of citizens' faces in real-time to be to obtain biometric face data, which can be compared to the biometric face information in the police 'watch list'. The court clarified that a 'biometric template' is created based on images from surveillance lists, which is used for algorithmic comparison with biometric data on natural persons attending to public events. The court stated that if the software detects a possible overlap between images captured by security cameras and a person on the wanted list, police officers will be notified to take appropriate actions (for example, arrest or interrogation of a person) [9].

It is worth noting above mention Court decision describe the process of automatic facial recognition, which involves the following steps (paragraph 9 of the Court of Appeal decision): 1) the compiling of an existing database of images. Images are processed to express "facial features" associated with objects in numerical values when using them for automatic face recognition; 2) capturing digital images of facial images is the method used to obtain a face image in real-time; 3) the software detects faces and highlights specific faces after the real-time surveillance camera captures footage; 4) facial extraction that leads to the software automatically extracting distinct

facial features from each face image, resulting in a biometric pattern that is exclusive to the image; 5) face comparison. By comparing the extracted facial features with images stored in the database, the program identifies any differences.; 6) comparison. Using the recognition program, a 'similarity score' is generated by comparing facial features in two images. The probability of matching faces is determined by this numeric value, with a high number indicating a higher chance of a positive match between two faces. A threshold is set to determine when an application inserts a match. The risk of a high false alarm rate can arise if the threshold is too low or too high (that is, the percentage of incorrect matches detected by the program) or thesystem has a high rate of false rejection when it comes to true matches that were not identified.

There are dynamic and statistical technologies for biometric identification. Dynamic based on the behavioural properties of the face, as: identification by typing text on the keyboard and writing text; by voice. Statistical identification is determined by the physiological features that a person has from birth, such as recognition of the eye iris and retina, thermogram, fingerprint, palm vein location, and DNA [10]. The use of identification by fingerprint, three-dimensional image of the face and iris of the eye are becoming more prevalent. Obtaining a fingerprint or iris scan involves using a special scanner to convert an image into a digital code and compare it with a previously entered link, which is also employed for reading.

**2. Limitations on privacy in time of remote identification and automated decision-making.**

The advancement of information and communication technologies for automated processing of personal data offers ample chances to control the lives of individuals. The overarching Internet and the accelerating pace of convergence between the physical and virtual spaces raise questions about redefining the existing balance between private and public in the life of an individual. It is important to recognize that the development of IoT, the processing of personal and metadata data by automated systems, comprehensive video surveillance, biometric remote identification and other types of intrusions into private life raise the issue of fair balance. Challenges posed by technological advancements prevalent the importance of following restrictive principles and the pursuit of a balance between private and public interest. In addition, the understanding of privacy differs in from state to state due to the variety of approaches to legal regulation of the Internet [11].

The balance between openness and closeness is currently shifting, with cross-border influences leading to an increase in transparency of information about an individual on the Internet. In the physical world, privacy conditions are observed as observance of certain boundaries (social, personal, or physical), which mean a real or imaginary separate boundary. However, the virtual world sees the gradual disappearance of boundaries. The way people perceive categories like 'distance' and 'personal space' is evolving. Privacy settings on social networks can create a false impression of personal environments when account data and personal preferences are shared with digital platforms and social networks. Social networks privacy conditions are unclear because users can restrict their ability to view their accounts, but the platform still has access to their account data.

An experiment conducted by the AOL organization in 2006 revealed that they published search queries from past periods to give the authors of the project an opportunity to investigate them. Having access to 650 thousand anonymized user data (IP addresses, usernames, search times, etc., replaced with individual numerical identifiers), a journalist identified a number of users within a few days by matching individual requests [12]. According to the survey results, society

has an expectation: disclosure of an increasing amount of personal data to state bodies and corporations that are interested to use them; privacy will become the prerogative of individuals possessing a resource for protection from mass surveillance; complexity of ensuring the security of personal data [13].

Yu. S. Razmetaeva states that two trends have been observed: a shift towards openness and anonymization in the public virtual space, and a shift towards the growing accumulation of personal data in global and local networks [14].

According to A. de Hingh, there is a gradual shift towards restricting privacy when it comes to the acquisition of personal data from civil circulation [15].

According to the definition of V.M. Bryzhko and V.G. Pilipchuk, guarantees of ensuring of privacy, in relation to personal data, are not absolute, significantly depend on the context. The restriction of privacy is determined by the norms of protecting private life and the requirements for disclosing personal data in public and private interest. The boundaries of information privacy are not stable, and a natural person can decide what data to report about themselves upon request [16]. P.D. Guiwang notes that a component of a person's private life are elements of private life, which can have both signs of privacy and public nature. The distinction is somewhat ambiguous, as a person may perceive certain aspects of labor participation, training, and other social activities as part of his or her personal life [17]. The scientist emphasizes the significance of balancing private and public interests in the ECHR's established practice. On the one hand, a person has the right to respect for private and family life under Article 8 of the ECHR. On the other hand, in cases of priority of public interest and the need to ensure the right of access to public information the right to private life may be a restricted the under Article 10 of the ECHR.

Due to competition on the one hand – the interests of a person in the protection of privacy and personal data, on the other hand – the interests of society in the processing of personal data in the public interest, the state is obliged to determine and maintain a balance of interests.

States have both positive and negative obligations to guarantee respect for the rights enshrined in Article 8 of the ECHR. The ECHR's decisions emphasize that restricting the right to privacy should be done according to law, with a legitimate objective, and be necessary in a democratic society.

Until now, in the practice of the ECHR, the boundaries of both positive and negative obligations of the state provided for in the ECHR have not been clearly defined. However, similarities can be identified in the principles applied. According to The Court decision in Palomo Sanchez and Others v. Spain the state's discretion should be used to strike a fair balance between the competing interests of individuals and society as a whole when dealing with disputes [18].

The exercise of individuals' right to information privacy and individual powers is subject to restrictions in Article 23 of EU Regulation 2016/679. These restrictions can be justified on the following grounds: national security; defence; public safety; prevention, investigation, detection and prosecution of criminal offenses or execution of criminal penalties, encompassing countering threats to public security and their prevention; significant objectives in the general public interest of the Union or a Member State, particularly crucial economic or financial interests of the European Union or a Member State, including monetary, budgetary and tax matters, social health and public safety; protection of the independence of the judiciary and protection of judicial proceedings; prevention, investigation, detection and prosecution of violations of ethical standards of regulated professions; monitoring, control and regulatory functions related, even periodically, to the exercise of the powers of public authority in the instances provided for in paragraphs (a) to

(e) and (g); (i) protecting the data subject or the rights and freedoms of others; (j) enforcement of rulings on civil claims.

According to Regulation EU 2016/679, if a normative legal act restricts the exercise of rights of individuals, it must have a specific reservation regarding: the purpose of processing and the category of personal data that is processed; the amount of restriction imposed; guarantees against abuse or unauthorized access or transfer; definition of controllers; terms of storage and application of guarantees, taking into account the scope, purpose and purpose of processing or category of data; risks to the rights and freedom of data subjects; and the rights of data subjects to obtain information on restrictions, to the extent that this does not harm the purpose of the restriction.

By connecting CCTV cameras to the Internet there is a risk of attackers gaining unauthorized access. The risks that come with accessing cameras connected to the Internet are constantly present. Most common way to prevent unauthorized access is to perform maintenance, update software, use encryption and encoding tools.

Automated face recognition technology can use video recordings taken with a video surveillance camera as personal data carriers. Currently, China is the leader in the use of video surveillance technology with remote biometric recognition, where remote biometric identification technologies are actively used and exported [19]. The technology allows for the assignment of points and a rating to a person in the system and can send information to law enforcement agencies in the event that the system shows that a natural person has violated the law. For instance, he has outstanding fines, is not paying alimony, or is being sought [20]. This means that the Chinese government can gather vast amounts of data on its citizens thanks to technology.

The iBorderCtrl project uses artificial intelligence at the external borders of the EU. The process involves compiling a traveller profile based on a computer-based automatic interview captured by the traveler's camera prior to the adventure, and analysing 38 micro poses with artificial intelligence. Currently this program is tested in Hungary, Latvia, and Greece [21]. The pilot project iBorderCtrl has not been approved for law enforcement bodies and is operated on a voluntary basis on the Hungarian, Greek, and Latvian borders.

Human rights organizations are currently using video surveillance technology with remote biometric recognition to identify victims of the slave trade and determine their location. The Amazon Recognition service's programs are used by Marinus Analytics, as an example [22].

However, the European Parliament call to ban using facial recognition databases like Clearview AI. Law enforcement agencies are being urged by the European Parliament to refrain from using private facial recognition databases like Clearview AI. Nevertheless, Ukraine was granted access to the private Clearview AI database, which has nearly ten billion photos, due to the Russian Federation's full-scale invasion, which enables individuals to be checked before crossing the border [23]. According to Ukrainian lawyer G.A. Mamedov, Ukrainian investigators are aided by the Clearview AI application in identifying potential criminals and those who have passed away [24]**.** In addition, Ukrainian law enforcement agencies are guided by the Berkeley Protocol when conducting investigating of violations of international criminal law using open digital data from the public domain. The Protocol was approved by the Office of the UN High Commissioner [25]. Clearview AI is a tool that was used by US law enforcement to identify rioters during the Black Lives Matter protests and the storming of the Capitol in Washington [26]. Clearview AI is known for offering services to public authorities and its representatives. Clearview AI collects photos from open sources, social networks on the Internet, in particular EU citizens. That's why the EU organization and regulators state that using Clearview AI violates EU

legislation. Since EU citizens' personal data is collected and processed by the program without their consent.

According to the European Parliament in the Resolution of October 6, 2021 remote biometric identification systems were recognized to have a positive impact on law enforcement agencies and judicial bodies in the fight against crime. Despite the risks of using the technology for mass surveillance. The use of systems for mass surveillance is considered be inappropriate at the same time [27].

Face recognition technologies pose a high risk of harm, as stated by the European Council for the Protection of Personal Data [28]. After all, comprehensive video surveillance, Internet of Things can affect both enjoyment of rights and well-being of natural person, and requires compliance with the legislation on the protection of personal data. The spread of technology poses an issue of the ethical and legal foundations of distribution and application of right.

Thus, the use of biometric identification systems requires compliance with the principle of legality. In addition, the risk of secondary use of data collected by video surveillance systems is exist, which contradicts the purpose of acquiring and collecting personal data. The effectiveness of technology is still under question, as video surveillance was not able to prevent terrorist acts on public transportation in London or the terrorist attacks in the United States [29]. K. Veliz confirms that the use of video surveillance systems is not effective in preventing terrorist acts, since they are not natural acts, but deliberate violations of the law. In addition, the interference with privacy that produces video surveillance also leads to the death of people [30].

Therefore, the positive effects of technology, restrictions on the widespread use of video surveillance systems with face recognition and the development of clear legal foundations for the use of technology are gaining momentum and becoming a trend in legal regulation. For instance, Facebook announced in 2021 that it will not use facial recognition technology, citing concerns from users and regulators [31]. It's possible that this decision was made because of scandals related to violation of personal data protection by the company in the EU [32]. Legislative restrictions on the use of technology are gradually being introduced in China. According to Art. 26 of the Law of the People's Republic of China on the Protection of Personal Information, which entered into force on November 1, 2021, the installation of equipment for collecting images or face recognition is required in public places for national and public security purposes. The collection of images and distinctive identification features may be carried out only for the purpose of national security, and may not be carried out for another purpose, except for the separate consent of the data subject [33].

In accordance with the Draft Law of Ukraine 'On a Unified System of Video Monitoring of the State of Public Security' the identification of an individual should be carried out on the basis of a data set: name; dates of birth or death; place of birth; sex; data on the registered place of residence (stay) of the person; information about citizenship; a digitized facial image; registration number of the taxpayer's registration card, etc., vehicle number, etc. [34], [35]. In order to rise effectiveness of the video surveillance system, the authorised state bodies will obtain access to the video surveillance systema and Unified State Demographic Register, the Unified Information, and Analytical System for Managing Migration Processes, the National Biometric Verification System, etc. The day before, the Ministry of Internal Affairs announced the launch of more than 50 thousand CCTV cameras, including those with facial recognition functions [36].

In some states of the US law enforcement agencies are increasingly restricting the use of face recognition video surveillance. The US Congress introduced a bill in the summer of 2020 that mandated a moratorium on the use of facial recognition and biometric technologies [37]. At the

state level, similar acts were adopted in Illinois, Texas, California, Washington [38], Colorado and Arkansas [39], Maine [40, 41], San Francisco, Oakland [42]. The primary reason for advocating for restrictions on technology use is the necessity to improve it because of the increasing cases of false recognition of individuals, which result in discrimination. Furthermore, the question arises of delegating decisions and functions to automated systems in the military sphere, which addresses the proposal to prohibit the use of military robots that can make fully automated decisions about human life and death [43]. Amnesty International calls for a ban on the use of facial recognition systems [44].

In accordance with the European Parliament resolution on Artificial Intelligence in Criminal law and its use by the police and judicial authorities in criminal matters a person not only has the right to correct identification, but also the right not to be identified at all. An exception may be made if it is necessary by law to protect public interests pursuant to paragraph 8 of the law [27].

According to experts, the face recognition system has shortcomings in its functionality, and analyzing individual facial features of a person can lead to random coincidence. There are known cases when the Chinese facial recognition system issued a fine for crossing the road at a red light to the head of a large air conditioning company, along with this, the violator was not at the scene of the accident. The camera captured an advertisement featuring a portrait of a businesswoman on a bus that was passing at the intersection at that time. Meanwhile, the automated system displayed the woman's ID number and her portrait on the screen near the intersection, indicating that the woman had violated traffic rules [45].

According to the Opinion of the European Council for the Protection of Personal Data and the European Supervisory Authority for the Protection of Personal Data on the EU Bill on Artificial Intelligence, that remote biometric identification of individuals in public places carries high risks of interference with the private life of individuals and may affect human dignity and calls for a general ban on any use of AI for automatic recognition of human traits in public places [46].

A similar position was expressed by the European Parliament in the Resolution on Artificial Intelligence in Criminal Proceedings and its use by the police and judicial authorities in criminal cases of October 6, 2021.

The European Parliament advocates for a permanent prohibition on the use of automated analysis and/or recognition in public places where human characteristics, such as gait, fingerprints, DNA, voice, and other biometric and behavioral signals, are present. Parliament is requesting a moratorium on the deployment of facial recognition systems that identify individuals for law enforcement purposes. Exclusions are allowed by law enforcement for identification purposes in the following situations and conditions: strict use for the purpose of identifying victims of crimes, observance of fundamental human rights, the obtaining results will be objective and free from discrimination, the law provides for strict guarantees against abuse and strict democratic control and supervision, and until empirical results appear.

The European Parliament's resolution on Artificial Intelligence in Criminal Proceedings and its use By the Police and Judicial Bodies in Criminal Cases, released on October 6, 2021, highlights the significance of video surveillance with remote face recognition. The technology could pose a threat to the right to human dignity and fundamental rights, which is guaranteed by the Charter of Fundamental Rights of the EU. The use and collection of any biometric data for remote identification purposes, for example, by facial recognition in public places, as well as at automatic checkpoints that are used for border control at airports, can pose high risks to fundamental rights. Depending on their intended use, context, and scope, the consequences of using these technologies

can be significantly different [47]. The European Parliament Resolution adheres to the belief that the introduction of AI systems in law enforcement and judicial spheres should be considered not as a simple technical possibility, but as a decision that affects the future implementation of human rights and freedoms, as well as the effective implementation of criminal justice. Law enforcement agencies should restrict the use of facial recognition systems to justifiable reasons, based on the principles of proportionality and necessity, and the relevant legal regulations. Technology must adhere to processing principles such as minimizing data, accuracy, restricting storage, data security, and accountability, as well as being legal, fair, and transparent, and pursuing a specific, explicit, and legitimate goal clearly defined in the legislation.

The use of video surveillance technology with facial recognition entails the processing of personal data and necessitates respect for both the principle of legitimate personal data processing and the principle of legitimate purpose of processing.

As a result of the use of facial recognition technology, a natural person cannot affect the amount of personal data collected in relation to him or her. This situation has the potential to harm his or her information self-determination, human dignity and privacy. In such conditions, the expansion of video surveillance technology usage can impact on individuals' decision-making, both when it comes to daily transactions and political choices. Furthermore, the objectives that are being pursued by video surveillance may remain unattainable, but privacy will be inevitably violated.

### 3. Risks of automated decision-making systems.

If the automated decision-making system, also known as the 'black box', is not transparent in its functionality, a person will be vulnerable and there will be risk of discrimination. After all, only a human being is capable of paying attention to the non-obvious motives for committing a crime and evaluating personal factors that the artificial intelligence system is not able to take into account.

The problem of biases in algorithmic systems are noted in the European Parliament Resolution on AI [48]. The essence of an algorithmized machine learning system is similar to a poisonous fruit tree. If the wrong steps are immediately committed, the entire chain, the resulting fruits, and the derived output will be poisonous. The obtained consequence generated machine learnings determined by the primary data sets. This means that both high-quality and low-quality data are fed to a machine learning system.

Furthermore, the algorithmized system reproduces the values and viewpoints that have already been assigned to someone in society. This is especially true when the logic of the machine learning system is unclear and the data that the system processes is unknown. In the end, such a viewpoint and values become an etalon in this system.

E. Dunham, the UK Information Commissioner's head, observed in 2021 that due to the exponential growth of personal data flows and evolving information technologies, data has become a significant asset that requires investment in management, protection, and respect to unlock its influential value. Proper data protection ensures that innovation works not only on paper, but also in the real world. Members of society may trust that companies and governments will process and collect their personal data. Trust is the fundamental element of data protection. The 1970s saw the start of data protection legislation, which is associated with trust, due to concerns that new technologies would be lost if innovations were not implemented. This trust-based relationship is still in place today. Planned data-driven innovations will only function successfully if people are willing to share their data, confident that it will be used fairly [49]. Thus, now, the key factor in the development of technology is transparency and trust. It's important to remember that not only

the real risks of using technology are significant, but also the hypothetical risks that people think exist, which can decrease users' confidence in using technology.

Similarly, it is noted in the UNESCO Recommendations on the ethical aspects of Artificial Intelligence that the development of AI-based systems raises ethical questions, in particular, regarding their impact on decision-making processes,... in various spheres of society and respect for human rights and fundamental freedoms, including freedom of expression, inviolability of private life and lack of discrimination [50].

In any society, standards and patterns exist, but in algorithmized systems, biases are elevated to a high degree and are capable of leading to negative consequences.

Tay is an example of a Microsoft chatbot that can be observed. The Chatbot learned to communicate with real data on Twitter by analyzing and participating in communication with Twitter users. In the end, Tay showed angry racist behavior, expressed intolerance and hostility. The fact that Tay reflects all the negative features that are inherent in users when communicating on the network makes it a failure in some ways. After all, algorithms study the structural biases and inequalities of society and reflect these forms of discrimination and victims who suffer most from them [51].

Accordingly, the designated model of behavior, the algorithm perceived as dominant, and with that, and reproduced in a higher degree. In the rest, Microsoft developers removed the chatbot and apologized. The above illustrates that specialists must take into account any predisposition introduced into the standard when developing systems.

In this sense, interest is attracted by the research of D. Chen who analyzes the possibilities and ways of using machine learning systems to identify and prevent biases in the judicial system. The scientist conducted a study by analyzing the decisions of US judges. The scientist suggests that there are two types of negative phenomena that can be identified: when judges do not take into account the legally significant circumstances of the case, and when judges do not take into account circumstances that have no legal significance or impact. It may not even be significant circumstances that relate to the case, but the time of day, weather, results of football matches, the birthday of the judge and his family and other circumstances. The adoption of court decisions and their results are influenced by all of these factors. Through the use of algorithms, the scientist divided the judges in the group based on the level of probability to predict the final decision they make. The first group was represented by those who had a high level of predictability, a final decision, and were influenced by external factors without delving into the essence of the case. The second group was presented by those with low predictability. T. Shep stressed once again that if the data processed by the algorithm encompassed structural biases from the beginning the output will also have a biased solution [52]. This study gives examples of biases that are inherent in judges. This algorithmic analysis example is significant and can be utilized to warn against the possibility of making a biased decision, highlight, teach, and recall current, probable biases. The conclusion can be made that algorithmic analysis and a machine learning system can assist in the identification of biases.

The algorithmic structural biases are reflected biases that exist in reality, and an automated system can detect and reproduce them. Along with the structural biases of algorithms, automation biases not only reproduce the biases of the physical world, but also actually affect the human way of thinking and decision-making, even when a person realizes that they are facing with prejudice. Automation biases – the tendency to over-rely on algorithm decisions [53]. In the time of the coronovirus outbreak, the face recognition system was installed on the city's transport structures

and recognized a person as wanted by police. Police officers detained the individual and the shortcomings of such detention were obvious to everybody, as the detained person was not the one on the wanted list. It was clear that the detained person was not a wanted one, yet the automated system recognized as it is. Automation biased were manifested in the fact that police officers, even understanding the absurdity of detention, preferred to trust the decision of the machine, rather than their own eyes, objective sense and justice.

The consequences of prejudice include uncertainty of functioning the 'black box' system works and obscurity of the algorithmic decision making. As result people try to bring any logic into the decision made by the algorithm. An attempt to fit a plausible logical explanation under the decision of the algorithm that has no reasonable justification, American experts are invited to call – algorithmic or mathematical laundering ('mathwashing' or 'farewashing'). In other words, algorithmic or mathematical laundering happens when a person ceases to trust himself, but automatically chooses to trust the program, neglecting critical thinking. F. Benenson, former head of the Kickstarter data department, noted that mathematical laundering occurs due to the excessive idealization of the effectiveness of algorithms [54]. T. Shep provides a distinction between mathematical washing that happens accidentally and that which happens purposefully. The washing is accidental, and a person does not intentionally capture the plausibility of an algorithm's decision, but they usually don't comprehend the vulnerability of an algorithmic system's decision. The washing occurs initially when individuals adhere to an obviously biased decision made by the system. The reason for purposeful adherence to an obviously biased decision may be due to a fear of public condemnation and a desire to protect their reputation, despite the apparent bias of the algorithm's decision in society [55]. The problem arises with the understanding of bias as such, since the standard of bias does not exist and depends on historical, territorial factors, social group, religious affiliation, gender, etc. For example, 100 years ago it was not recognized as a bias to prevent women from certain professions, positions, or deprivation of the right to vote, since this was a common situation for that time. However today, the establishment of any restrictions on women's employment of certain positions or certain activities is considered bias. In most civilized states around the world, bias can be seen in the fact that different levels of human rights are determined by religion. The main condition of the development the automatic algorithm is to ensure equal rights and attitudes to the person who belongs to the different social groups.

Thus, the developers' values and culture have an impact on the functionality of the algorithm. According to N. Bostrom and E. Yudkovsky's statement, if Archimedes participated in the development of the algorithm, the results would be influenced by ancient Greek values, structures, and ethical norms, in particular, the acceptance of slavery [56].

Therefore, as A.E. Radutny, who studies Big Data in criminal law, notes, correlations based on the processing of Big Data can: influence on the decisions made by a person; to supplement the argumentation to justify decisions made by a person; contradict the decisions made by a person in view of the knowledge and experience gained [57]. When making significant legal decisions, it is important to consider that the final decision should be made by a human being because the system can provide biased and inaccurate assessments and predictions.

Summarizing the above, we propose to distinguish: structural biases, which are a consequence of the functioning of the algorithm, are the result of data analysis, the output of the analyzed data to the reference level; and algorithmic biases, due to the fact that a person overly relies on the decision to make an algorithm, neglects his own experience and his own eyes.

People tend to rely on automated systems solutions too much, disregarding their own judgments, which is why Advocate General Pikamäe's opinion is important. The preliminary recommendation decision of the automated system can have an impact on the individual in particular. General Counsel Pikamäe expressed judgment in the SCHUFA Holding and Others case that the decisive factor is the effect that the "decision" may have on the person concerned. If the person is 'in the know', the organization using the automated decision-making system should consider whether other previous, fully automated steps could themselves lead to legal consequences or have significant impact on the data subject. Pikamäe states that the automated credit score calculation for SCHUFA Holding and Others can already serve as a solution for the purposes of Art. 22 (1). And this despite the fact that the final decision on the loan is made with the participation of a person who can reasonably be classified as "significant decisions." The impact of the 'decision' on the person concerned is the decisive factor. Since a negative credit score in itself can have adverse consequences for the person concerned, namely, to significantly restrict it in the exercise of its free rights or even to stigmatize it in society, it seems justified to qualify it as a 'decision' in the sense of the above provision, i.e. Article 22 (1), when a financial institution gives it priority in its decision-making procedure. Indeed, in such circumstances, the applicant for a loan is affected from the moment of the assessment of its creditworthiness by the creditworthiness verification company, and not only at the final stage of the decision. Indeed, in such circumstances, the applicant for a loan is affected from the moment of the assessment of its creditworthiness by the credit checking company, and not only at the final stage of the refusal to issue a loan, when the financial institution does not apply the result of this assessment to a particular case [58]. At present, the final decision in the case has not yet been made, however, being potentially significant, it should introduce some legal certainty for the legal community regarding the application of automated decision-making systems, data protection and the rights of data subjects.

The legality of decisions made with the help of algorithms is becoming the subject of consideration in the courts of the USA. In Houston, the results of secretly applying an algorithm to assess the performance and influence of teachers on students were used to dismiss teachers. The used algorithm was part of an educational teacher rating system created by technology firm SAS, which treated the algorithm and software as a trade secret. Details of the system's operation and performance evaluation were not disclosed. According to the court decision the system did not explain how the teacher to increase the rating. The court ruled on the violation of the rights of teachers, due to the unreasonableness and opacity of the decisions by the system [59].

One of the more challenging tasks involves explaining the decision made by the algorithm.

In the U.S. criminal justice system at its various stages introduced more than 60 automated systems. The well-known are following: algorithm PSA (Public Safety Assessment) or COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), which is used in decision-making [60]. The use of algorithms to predict human behavior is criticized since the prognostic results do not give the true truth by 100%, and the approximate predictability ranges around 65%. The right to a fair trial cannot be realized if the judge uses the prognostic algorithm to decide on the merits of the case, particularly if they try to implement the algorithm's recommendation literally [61]. In particular, the problem of an overloaded judicial system concerns both Ukraine and the United States. Therefore, a person could face with a high temptation to use the proposal generated by the algorithm. The goal of using algorithms in the judicial system was to unload it. The State vs Loomis case, considered by the Wisconsin Supreme Court in 2017,

is an example of how such decisions become objects of appeal when they have an impact on the rights of individuals, as demonstrated by the analysis.

Defendant Eric Loomis appealed the verdict to the Wisconsin Supreme Court using an algorithm, demanding a review of the decision and the use of the algorithm. The program analyzes the individual facts and circumstances of the case and gives the accused a certain assessment, taking into account which the judge can soften or strengthen the decision. The accused do not have access to the program and cannot obtain an explanation of the factors for which they are given the status of 'dangerous to society'. Moreover, the algorithmic decision-making technology COMPAS, which is employed in the United States, is kept secret and not divulged by either the accused or the judge. With that, Loomis was denied clarification of the decision. Representatives of the accused in court argued that the COMPAS program is imperfect and accepts very generalized conclusions. The future behavior of the individual is predicted by analyzing data like gender and age, and non-disclosed criteria are used to evaluate the defendant.

The court was confronted with the question of the permissible restriction of using algorithms to predict the subject's behavior. The Court observed that the algorithmic assessment should not be primary consideration and other reason should take into account. However, under any circumstance, the decision should be motivated by reference to the use of tools and factors in justifying the decision. The court noted that the rights of E. Loomis are respected if the court decision is not solely determined by the algorithm's assessment [62,63].

## Conclusions

The article presents a brief statement on the challenges faced by privacy in the context of the AI, specifically regarding the automated decision-making process and video surveillance with remote face recognition. Using algorithms poses a problem due to the lack of ability to establish the foundation for decision-making algorithms and the presence of biases. The growing scale of biases makes it more challenging to follow and enforce the rule of law in the context of autonomous systems development. Prejudice's impact is enhanced by the invention of automated decision systems and Big Data, as demonstrated by examples of the United States. This situation is due to the fact that the system relies on biases that exist in reality. The essence of an algorithmized machine learning system may be compared to a poisonous fruit tree.

Despite the fact that the final decisions in finance and judicial field are made with the participation of a natural person, the effect that the decision of an automated system has on the relevant data subject can have adverse consequences for the person.

It is established that bias is not defined, and biases can differ depending on the context, historical factors, territorial factors, social group, religious affiliation, gender, and other factors.

The Regulation EU 2016/679 offers dependable security against automated decision-making, but it could be ineffective in its present form. There is a deficiency in implementing transparency and accountability principles due to the widespread use of automated decision-making systems and automated data processing to support human decision-making.

EU legislation mandates that economic entities refrain from making decisions about individuals solely based on automated processing of personal data, which is decision-making by an AI system. The controller is obliged to take measures to prevent decisions based on data on race, ethnic origin, political beliefs, religion, membership in a trade union organization, genetic predispositions, health or sexual orientation.

Societies and the legal system are facing challenges in ensuring equal rights and attitudes for people belonging to different social groups due to the development of an automatic algorithm.

## REFERENCES


1. ISO/IEC JTC 1/SC 37 Biometrics URL: https://www.iso.org/ru/committee/313770.html (Accessed: 22 April 2025).
2. Pro Yedinij derzhavnij demografichnij reyestr ta dokumenti, sho pidtverdzhuyut gromadyanstvo Ukrayini, posvidchuyut osobu chi yiyi specialnij status Zakonu Ukrayini. Vidomosti Verhovnoyi Radi. [On the Unified State Demographic Register and documents confirming the citizenship of Ukraine, certifying the identity or its special status of the Law of Ukraine. Information of the Verkhovna Rada]. 2013, 51, st.716.
3. Bryginets, C.C. (2019) Biometrichni dani: zbir i zahist u Yevropi, SShA ta Ukrayini. Yuridichna gazeta. [Biometric data: collection and protection in Europe, USA and Ukraine. Legal newspaper]. 40 (694). URL: https://yur-gazeta.com/publications/practice/inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html (Accessed: 10April 2025).
4. Postanova vid 19.09.2018 № 806/3265/17 Verhovnij Sud. Velika Palata [Resolution. the Supreme Court. Grand Chamber]. URL: https://verdictum.ligazakon.net/document/76822787
5. Guidelines 3/2019 on processing of personal data through video devices Adopted on 29 January (2020). URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (Accessed: 22 April 2025).
6. Opinion 4/2007 on the concept of personal data. Data Protection Working Party. 01248/07/EN WP 136. URL: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf
7. Act UK Personal Data Protection Act (2018). URL: https://www.legislation.gov.uk/ukpga/2018/12/contents
8. R (on the application of Edward BRIDGES) v The Chief Constable of South Wales Police in the Court of Appeal (civil division) on appeal from the high court of justice queen's bench division (administrative court) Cardiff District Registry Case No: C1/2019/2670. 11.08.2020 UKR: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf (Accessed: 22 March 2025).
9. Equality Act. (2010) URL: https://www.legislation.gov.uk/ukpga/2010/15/contents
10. Bidyuk, P., Bondarchuk, V. (2009) Suchasni metodi biometrichnoyi identifikaciyi. Pravove, normativne ta metrologichne zabezpechennya sistemi zahistu informaciyi v Ukrayini. [Modern methods of biometric identification. Legal, regulatory and metrological support of the information protection system in Ukraine]. 1(18), 137-146.
11. Rainie, L., Anderson, J. (2014) Privacy in 2025: Experts' Predictions. / USA, Pew Research Center. URL: http://www.pewinternet.org/2014/12/18/privacy- in-2025-experts-predictions/ (Accessed: 22 March 2025).
12. Barbaro, M., Zeller, Jr.T., (2006) A Face Is Exposed for AOL Searcher No. 4417749 URL: https://www.nytimes.com/2006/08/09/technology/09aol.html(Accessed: 22 March 2025).
13. Madden, M. (2018) Public Perceptions of Privacy and Security in the Post-Snowden Era URL: https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/ (Accessed: 13 March 2025).
14. Razmetaeva, Y.S., (2020) Cifrovi prava lyudini ta problemi eksteritorialnosti v yih zahisti. Pravo ta derzhavne upravlinnya, [Digital human rights and problems of extraterritoriality in their protection. Law and public administration]. 4, 18-23.
15. De Hingh, A.E. (2018) Some Reflections on Dignity as an Alternative legal Concept in Data Protection Regulation. German Law Journal, 19(5) 1274.
16. Brizhko, V.M., Pilipchuk, V.G. (2020) Privatnist, konfidencijnist ta bezpeka personalnih danih. Informaciya i parvo [Privacy, confidentiality and security of personal data. Information and law]. 1(32), 33-46.
17. Gujvan, P.D. (2019) Nedotorkannist danih pro osobiste zhittya lyudiniyak element yiyi pravana privatnist. Chasopis Kiyivskogo universitetu prava. [The inviolability of data on the personal life of a personas an element of her right privacy. Journal of Kyiv University of Law]. 4, 179-183.
18. Decision of the Grand Chamber of the European Court in the case of Palomo Sanchez and Others v. Spain (Palomo Sanchez and Others v. Spain).
19. U Kitayi kamera rozpiznala pidozryuvanogo sered 60 tisyach lyudej. (2018) [China camera recognized the suspect among 60 thousand people]. URL: https://volynonline.com/u-kitayi-kamera-rozpiznala-pidozryuvanogo-sered-60-tisyach-lyudey/ (Accessed: 10 March 2025).
20. Skanuvannya za hodoyu i formoyu tila: u Kitayi zapuskayut sistemu totalnogo stezhennya. 2018. [Scanning by gait and body shape: China launches total tracking system]. URL: https://konkurent.ua/publication/32528/skanuvannya-za-hodou-i-formou-tila-u-kitai-zapuskaut-sistemu-totalnogo-stezhennya/ (Accessed: 23 March 2025).

21. Periodic Reporting for period 2 - iBorderCtrl (Intelligent Portable Border Control System URL: https://cordis.europa.eu/project/id/700626/reporting
22. Kaiser, L.M., (2018) Analytics fights human trafficking using Amazon Rekognition09 AUGURL: https://aws.amazon.com/blogs/machine-learning/marinus-analytics-fights-human-trafficking-using-amazon-rekognition/ (Accessed: 10 March 2025).
23. 10 milyardiv foto i sistema rozpiznavannya: Ukrayina otrimala dostup do bazi Clearview AI. (2022) [10 billion photos and recognition system: Ukraine gained access to the Clearview AI database]. URL: https://www.ukrinform.ua/rubric-technology/3429032-10-milardiv-foto-i-sistema-rozpiznavanna-ukraina-otrimala-dostup-do-bazi-clearview-ai.html(Accessed: 29 March 2025).
24. Mamedov, G.A. (2022) Cifrova kriminalistika. Yak ce dopomoglo zibrati dokazi zlochiniv u Buchi? [Digital forensics. How did this help gather evidence of crimes in Bucha?]. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html (Accessed: 27 March 2025).
25. Protokol Berkli z vedennya rozsliduvan z vikoristannyam vidkritih cifrovih danih zatverdzhenij Upravlinnyam Verhovnogo komisara OON. Centr prav lyudini. Yuridichna shkola Kalifornijskogo universitetu Berkli. 2020 r. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (Accessed: 27 March 2025).
26. Goda M. Clearview AI zbiraye bazu fotografij vsih zhiteliv planeti: dlya chogo ce potribno kompaniyi. [ Clearview AI collects a database of photos of all the inhabitants of the planet: why the company needs it]. URL: https://24tv.ua/tech/clearview-ai-zbiraye-bazu-fotografiy-vsih-zhiteliv-novini-tehnologiy_n1870807 (Accessed: 28 March 2025).
27. European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) 6 October 2021UR: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html (Accessed: 25 April 2025).
28. Trainees Conference Recording – An. An Orwellian Premonition: a discussion on the perils of biometric surveillance. URL: https://edps.europa.eu/press-publications/press-news/videos/trainees-conference-recording-orwellian-premonition-discussion_en (Accessed: 22 March 2025).
29. London bombings of 2005 URL: https://www.btp.police.uk/police-forces/british-transport-police/areas/about-us/about-us/our-history/london-bombings-of-2005/
30. Veliz, C., (2021) The Power of Big Tech and Ethics, GRC World Forumshttps://www.grcworldforums.com/on-demand-content/the-power-of-bigtech-and-ethics-carissa-veliz/1185.article
31. Pesenti, J. (2021) Intelligence An Update On Our Use of Face Recognition. URL: https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/(Accessed: 22 March 2025).
32. Balowskiak, N. Starshij brat bilshe ne stezhit za toboyu. Chomu demokratichni krayini vidmovlyayutsya vid tehnologij rozpiznavannya oblich. [The elder brother no longer watches you. Why democracies are abandoning facial recognition technologies]. URL: https://chas.news/future/starshii-brat-bilshe-ne-stezhit-za-toboyu-chomu-demokratichni-kraini-vidmovlyayutsya-vid-tehnologii-rozpiznavannya-oblich (Accessed: 7 March 2025).
33. Personal Information Protection Law of the People's Republic of China, PIPL URL: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021 (Accessed: 8 March 2025).
34. V Ukrayini vvedut sistemu videonaglyadu za gromadyanami i zvirki yih danih dlya identifikaciyi – u tomu chisli pro misce prozhivannya. 9 VERESNYa 2024. URL: https://sud.ua/uk/news/publication/310121-v-ukraine-vvedut-sistemu-videonablyudeniya-za-grazhdanami-i-sverki-ikh-dannykh-dlya-identifikatsii-v-tom-chisle-o-meste-prozhivaniya (Accessed: 9 March 2025).
35. Proekt Zakonu pro yedinu sistemu videomonitoringu stanu publichnoyi bezpeki № 11031 vid 20.02.2024. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43733 (Accessed: 22 March 2025).
36. V Ukrayini zapuskayut Yedinu sistemi videomonitoringu stanu publichnoyi bezpeki, u tomu chisli – rozpiznavannya oblichchya. 16 sichnya 2024. URL: https://sud.ua/uka/news/publication/290740-v-ukraine-zapuskayut-edinuyu-sistemu-videomonitoringa-sostoyaniya-publichnoy-bezopasnosti-v-tom-chisle-raspoznavanie-litsa?fbclid=IwAR0_pXDJx43oMd9pL0JKnbwnAXffs1hAHaWROx9a4HFhjNBob_uxpbe532Y (Accessed: 26 March 2025).
37. The Facial Recognition and Biometric Technology Moratorium Act of 2020". Congress. gov. 2020. URL: https://www.congress.gov/bill/116th-congress/senate-bill/4084 (Accessed: 9 March 2025).

38. Elamroussi, A. (2021) This Washington county is the first to ban facial recognition technology, official says URL: https://edition.cnn.com/2021/06/02/us/facial-recognition-technology-ban/index.html (Accessed: 27 March 2025).
39. Avocat, M. (2020) Facial recognition regulation in the USA: an efficient legal patchwork?". URL: https://www.avocats-mathias.com/donnees-per- sonnelles/facial-recognition-usa. (Accessed: 12 April 2025).
40. Gershgorn, D. (2021) Maine passes the strongest state facial recognition ban yet. Jun 30, URL: http://https//www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/ (Accessed: 1 March 2025).
41. Maine Enacts Strongest Statewide Facial Recognition Regulations in the Country (2021) URL: https://www.aclu.org/press-releases/maine-enacts-strongest-statewide-facial-recognition-regulations-country (Accessed: 2 March 2025).
42. Cyphers, B., Schwartz, A. (2021) Sheard N. Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-time Tracking, and More. URL: https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification (Accessed: 5 March 2025).
43. Citron, D.K., Frank, A.P. (2014) The scored society: Due process for automated predictions, Washington Law Review, 89, 1–33.
44. Ban dangerous facial recognition technology that amplifies racist policing. (2021) URL: https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/ (Accessed: 1 March 2025).
45. Voinov M. Sistema rozpiznavannya oblichchya: pravovi aspekti vikoristannya v Ukrayini ta v YeS. [Face recognition system: legal aspects of use in Ukraine and the EU]. URL: https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes/ (Accessed: 6 March 2025).
46. EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) URL: https://edps.europa.eu/data-protection/our-work/publications/opinions/joint-opinion-edps-edps-proposal-regulation-european_en (Accessed: 22 April 2025).
47. Artificial Intelligence Act. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM (2021)0206 – C9-0146/2021 – 2021/0106(COD)) URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (Accessed: 10 April 2025).
48. Denham, E., (2021) How modern data protection is helping to unlock the power of data. Speech. URL: https://www.wired-gov.net/wg/news.nsf/articles/How+modern+data+protection+is+helping+to+unlock+the+power+of+data+13052021122500?open (Accessed: 2 April 2025).
49. YuNESKO. Rekomendaciya ob eticheskih aspektah iskusstvennogo intellekta. (2021) [UNESCO Recommendations on the ethical aspects of artificial intelligence that the development of AI-based systems]. URL: https://unesdoc.unesco.org/ark:/ 48223/pf0000380455_rus (Accessed: 10 April 2025).
50. Artificial intelligence: How does it work, why does it matter, and what can we do about it? 28-06-2020 URL: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)641547 (Accessed: 8 April 2025).
51. Chen, D.L. (2019) Machine Learning and the Rule of Law. Law as Data, Santa Fe Institute Press, ed. M. Livermore and D. Rockmore, 16. URL: https://ssrn.com/abstract=3302507 (Accessed: 7 April 2025).
52. Goddard, K., Roudsari, A., Wyatt, J.C., (2012) Automation bias: a systematic review of frequency, effect mediators, and mitigators, Journal of the American Medical Informatics Association, 19 (1), 121–127, https://doi.org/10.1136/amiajnl-2011-000089 (Accessed: 5 April 2025).
53. Byrnes, N. (2016) Why We Should Expect Algorithms to Be Biased. URL: https://www.technologyreview.com/2016/06/24/159118/why-we-should-expect-algorithms-to-be-biased/ (Accessed: 2 April 2025).
54. hat is mathwashing? URL: https://www.mathwashing.com
55. Bostrom, N., Yudkowsky, E. (2018) The Ethics of Artificial Intelligence. Artificial Intelligence Safety and Security. ed. by R. V. Yampolskiy. New York: Routledge, 57-69.

56. Radutnij, O.E. (2023) Veliki dani: korelyaciyi ta prichinnist (kriminalno-pravovij aspekt). Informaciya i pravo. Kiyiv:Nauk.-doslid. centr pravov. informatiki Nac. akad. pravov. nauk Ukrayini. [Big data: correlations and causality (criminal law aspect). Information and law. -Kiyiv: Scientific-research. center of law. Informatics Nats. acad. of law. Sciences of Ukraine]. (45), 94-112.
57. Opinion of Advocate General Pikamae delivered on 16 March 2023 (1) Case C 634/21 OQ v Land Hesse, Joined party: SCHUFA Holding AG. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=271343&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=8514846 (Accessed: 29 March 2025).
58. Webb S. Houston teachers to pursue lawsuit over secret evaluation system. May 11, 2017 URL: https://www.houstonchronicle.com/news/houston-texas/houston/article/Houston-teachers-to-pursue-lawsuit-over-secret-11139692.php (Accessed: 28 March 2025).
59. Herrschaft, B.A. (2014) Evaluating the reliability and validity of the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) URL: https://rucore.libraries.rutgers.edu/rutgers-lib/46260/#citation-export (Accessed: 28 March 2025).
60. G'sell, F. (2020) Les progres a petits pas de la «justice predictive» en France. ERA Forum, 21, 299-310.
61. State of Wisconsin v. Eric L. Loomis. July 1, 2016.Case № 2015AP157-CR URL: https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html (Accessed: 6 March 2025).
62. White Paper On Artificial Intelligence - A European approach to excellence and trust Brussels, 19.2.2020 COM (2020) URL: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf (Accessed: 2 April 2025).
63. Artificial intelligence: How does it work, why does it matter, and what can we do about it? 28-06-2020 URL: https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)641547 (Accessed: 15 March 2025).