Comparative Analysis of the AI Regulation of the EU, US and China from a Privacy Perspective

V. Gábor Rádi
Károli Gáspár University of the Reformed Church, Budapest, Hungary
radi.vilmos@gmail.com

Abstract - Artificial intelligence is already part of our everyday lives. We encounter it several times a day, when using a smartphone or social media, when shopping online, or even without any visible signs, such as in case of a secret facial recognition programme.
The area of data protection is closely linked to the evolution of technology, especially wit so-called 'disruptive' technologies raising new data protection issues and risks. Artificial intelligence also creates a new situation because, unlike other technologies, it is difficult to explain how it works and to predict the precise outcome of its use. Regulatory authorities detected the need of proper regulation which ensures both the technical advance and the protection of the natural person's private life.
This paper presents an overview of the major regulatory tools that have emerged in the field so far in the EU, in the US, and finally in China. However, the author of this paper finds that current regulation is rather 'fragmented'; the EU is the first one to come up with a comprehensive and wide-ranging regulation of AI; hopefully the others will follow its path with respect of privacy regulation as well..

Keywords: AI, data protection, privacy, US, China, EDPB.

I. INTRODUCTION

AI is one of the most interesting emerging technologies. As we hear day by day exciting news about the capabilities of artificial intelligence, more and more states or international organizations feel the necessity to create an effective regulation about the technology. My hypothesis is that there is currently no truly effective, comprehensive and wide-ranging legislation on AI that is already in place; or that the current legislation is "fragmented", with sub-areas and functions being the focus of legislators, and other actors stepping in with unified proposals in this area. In order to clarify this issue, I will examine the regulatory instruments that have been put in place so far, concentrating on the legal material of the three most powerful economies of the world: the US, the European Union and China.

II. AI REGULATION IN THE US

The US is probably the country which is taking the lead in the development of artificial intelligence; and several advanced AIs are coming out from US-based companies. Despite this fact, the regulation is still at it's first steps in the US; several pieces of legislation related to AI have been proposed at the federal level, which unfortunately have not yet been finally adopted. For example, the Algorithmic Accountability Act [1] and the Consumer Online Privacy Rights Act [2], which would have dedicated a specific chapter to algorithm-based consumer decision-making. More recent proposals are the Good AI Act of 2022 [3] which would establish an "Artificial Intelligence Hygiene Working Group"; and the Advancing American AI Act [4] intending to regulate the use of AI by governmental agencies. Both regulations were already introduced last year, but since then there has been no significant advancement. It can be said that there is currently no explicit comprehensive federal legislation on AI.

At this stage, it appears that the first major piece of federal-level AI legislation could be the American Data Privacy and Protection Act (ADPPA) [5], which is a „possible" federal-level privacy legislation, although it is also currently in the legislative process and has not been finalised. The draft generally designates the Federal Trade Commission (FTC) as the competent supervisory authority for data protection. The chapter on "Civil Rights and Algorithms" contains the regulation of interest to this paper: within 2 years of the enactment of the prospective legislation, it will require organizations managing large databases that use AI that may cause significant harm to individuals to: first, conduct a privacy impact assessment (based on criteria described in detail in the draft); and second, review the algorithm's architecture, design, structure and inputs, training data, to mitigate risks to the rights of data subjects. Impact assessment and review documentation must be submitted to the FTC within 30 days of their completion. The legislation also requires the FTC to conduct studies on the application of this section of the bill and to publish guidelines on the subject. As we can see, AI is only a minor part of the future ADPPA law.

To address this shortcoming of the lack of federal AI legislation, the White House Office of Science and Technology Policy released the Blueprint for AI Bill of Rights (Blueprint) [6] in October 2022. The Blueprint sets out 5 principles for the use of AI:

(a) building safe and effective systems;

(b) protection against algorithm-based discrimination;

(c) data privacy: concepts similar to GDPR such as "privacy by design", the exercise of data subjects' rights, and protection against abusive data practices are mentioned here;

(d) notice and explanation: data subjects should know when they are using an automated system and should also be informed of the impact of the automated system on them;

(e) human alternatives, and the possibility of consideration and fallback: the data subject should be able to opt-out of AI-based processing or, if they so wish, to request human intervention in the AI decision-making process.

Again, it is important to stress that the Blueprint is not a binding law, but only a recommendation for the development and use of AI.

At the end of the chapter, the author concludes that there is currently no meaningful AI regulation in the US, although significant progress is expected in the near future through ADPPA - however, the author does not expect the implementation of a comprehensive binding regulation as the one in Europe, which will be introduced below. In the US, there are also currently recommendations (the most important of which is the Blueprint) that set the direction for the development and use of AI.

III. REGULATION AND GUIDELINES AT EUROPEAN LEVEL

The first important piece of legislation on data protection is the General Data Protection Regulation (hereinafter GDPR) [7]. Article 5 of the GDPR provides for principles for the processing of personal data, of which the most prominent in the context of AI:

(a) transparency: ”Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”;

(b) purpose limitation: ”personal data [must be] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (…)”;

(c) data minimisation: data must be ”adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed";

(d) accuracy: the data used must be "accurate and, where necessary, kept up to date (...)".

Profiling is defined in Article 4 of the GDPR as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements ".

The concept of automated decision-making is briefly mentioned in the 71th section of the preamble of GDPR, stating it is a form of a „decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her”. The Article 29 Working Party WP251 Guideline [8] gives us more elaborated details: "Automated decision-making has a different scope and may partially overlap with or result from profiling. Solely automated decision-making is the ability to make decisions by technological means without human involvement. Automated decisions can be based on any type of data, for example:

- data provided directly by the individuals concerned (such as responses to a questionnaire);
- data observed about the individuals (such as location data collected via an application);
- derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score).

Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However (…) automated decision-making process could become one based on profiling, ()."

The GDPR places a strong emphasis on adequate information, thus, according to Articles 13(2)(f) and 14(2)(g), the data controller is obliged to provide information and according to Article 15(1)(h), the data controller is obliged to provide information to the data subject, at his or her request, on whether automated decision-making, including profiling, is taking place in relation to him or her. The data controller shall also inform the data subject at least of the logic used in such cases and of the comprehensible information relating thereto; and of the significance of such processing and the likely consequences for the data subject.

In order to protect the data subject, the GDPR sets limits on profiling and automated processing in Article 22:

"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9 (1) [of GDPR], unless point (a) or (g) of Article 9 (2) [of GDPR] applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

We can conclude automated functions are well-regulated, but it takes only a smaller piece of the GDPR.

Let’s look at some legal text specifically targeted on AI: On 25 January 2019, the Council of Europe issued its Guidelines on the relationship between artificial intelligence and data protection [9]. The declaration is

divided into 3 main parts: general guidance, advice for developers and advice to legislators and regulators. The Guidelines state that AI development should be in line with the so-called Council of Europe Convention 108 on Data Protection (or its modernised version) and accordingly sets out data protection principles and emphasises the rights of data subjects. For developers, it sets out a number of privacy-by-design principles, draws attention to the importance of ensuring that data subjects are always aware that they are communicating with AI, and calls for developers to establish independent bodies to be consulted on ethical issues in the development of AI. The final chapter of the declaration calls for the drafting of codes of ethics and witness mechanisms and stresses that human intervention should always be allowed. The chapter advocates that national supervisory authorities should have adequate resources to monitor AI developments and that different disciplines should cooperate on this issue; it also calls for developers to consult with supervisory authorities before creating AI that could have a significant impact on the rights of data subjects.

The European Commission have founded the High-level Expert Group on Artificial Intelligence (hereinafter referred to as AI HLEG) which serves as an advisory body to them. On 8 April 2019, the AI HLEG issued the "Ethical Guidelines for Trusted AI" [10], in which it identified 3 elements of trusted AI that must be met throughout the lifecycle of the system: a) it must be lawful; b) it must be ethical, i.e. ensure compliance with ethical principles and values; and c) it must be technically and socially robust.

The Guidelines also identified seven key requirements for ethical AI: human agency and human oversight; technical stability and security; data protection and data management (lawfulness); transparency; diversity, non-discrimination and equity; social and environmental well-being; and accountability. As we can see, the requirements of data protection, transparency and accountability are in parallel with the principles of the GDPR. The AI HLEG subsequently issued a guidance note for stakeholder organisations and individuals (”Assessment List for Trustworthy Artificial Intelligence (ALTAI)”) for self-assessment [11] on 17 July 2020, which can be used to determine the extent to which the AI they are developing or applying can be considered trustworthy. The guide asks questions along the 7 requirements that can be used for self-assessment, so that requirements relevant to data protection are also included.

The White Paper On Artificial Intelligence - A European approach to excellence and trust [12] published by the European Commission summarizes the desired goals, risks and partially repeats the former documents of AI HLEG mentioned above. The White Paper states that its goal to achieve both an ”ecosystem of excellence” and an ”ecosystem of trust” while also highlighting the main problems:

- risks for fundamental rights, including personal data and privacy protection and nondiscrimination and
- risks for safety and the effective functioning of the liability regime.

The White Paper outlines the scope of future compulsory regulation, mentioning the high-risk AI and emphasizes the requirements set up earlier by AI HLEG, and also elevates privacy into the important topics.

The EU binding legal act currently exists only in draft form: the ”Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts” [13] was presented on 21th of April, 2021. The proposed legislation aims to make Europe a global centre for trusted AI. As The draft AI Act requires the below listed criteria to be met for a software to be identified as AI: a) the AI must use specific technologies listed in Annex I of the AI Act; b) it must be able, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations; or c) it must be able to produce outcomes that "influence" the environment.

The draft AI Act classifies AI programmes into several categories based on a risk approach:

The first group includes AI systems that pose unacceptable risks, or otherwise "prohibited", and that clearly threaten the safety, livelihood and rights of people and will therefore be banned. Examples of such programmes include: those that manipulate human behaviour to circumvent the free will of users, or those that allow "social scoring" by governments.

At the other end of the scale are "not high risk" schemes, which can be further broken down into two sub-categories. The first category includes "minimal-risk AI" programmes, the use of which poses almost no risk to the rights and security of users; these are not covered by the AI Act. The second sub-category is the group of "limited-risk AI", where only basic requirements are included (the requirement of transparency: when interacting with a system, users must be aware that they are interacting with a program and can decide whether to continue or discontinue the activity on that basis. Examples of AIs with limited risk are chatbots or deepfake programs.

Most of the draft AI Regulation deals with the last category, so-called "high-risk" AI. The categorisation is set out in the Annexes II. and III. of the AI Act, and – amongst others – includes AI used in the following areas: biometric identification of natural persons; critical infrastructure (e.g. transport) that may endanger the life and health of citizens; education or training (e.g. exam scoring); employment (e.g. CV sorting software); essential private and public services (e.g. assistance assessment, credit scoring); law enforcement (e.g. polygraph AI analysis, personal risk analysis, evidence reliability assessment); asylum and border control (e.g. document authentication); justice and programmes used in democratic processes (e.g. application of laws to specific facts).

For high-risk AI systems, the AI Act sets out a number of requirements: a risk management system must be implemented and risk management measures must be developed in accordance with the criteria described in the draft; the data sets implemented into the software must be of high quality and accurate; technical documentation

must be prepared containing the elements described in the relevant annex of the AI Act, including the information on the AI and its purpose that the authorities need to assess the adequacy of the system; logging of events for subsequent traceability and traceability; clear and adequate information to users about the AI; ensuring adequate human supervision; and finally, the requirement for accuracy, stability and cyber security. As can be seen, the requirements are in line with the expectations of the GDPR in a number of respects, and the GDPR compliance of AI systems will also help to meet the requirements set out in the draft. The AI Act imposes specific obligations on "manufacturers" as well as on importers, distributors and users. The draft imposes a number of detailed rules on the standards, certificates, conformity assessment processes and assessment bodies that will be required in the future, as well as their registration and notification to the public.

The AI Act probably will be an important step from a privacy perspective as well, because it mentions the relationship between the regulation of AI and data protection at several points. In this context, the European Data Protection Supervisor (hereinafter "the Supervisor") is given a number of powers: under Article 53, she or he is empowered to create a regulatory "sandbox" for AI facilitation, for a limited period of time, the development, testing and validation of innovative AI systems before they are put into service. The Supervisor is a permanent member of the European Artificial Intelligence Board under Article 57. Under Article 59, the Supervisor acts as the competent authority for the supervision of the AI aspects of the EU institutions falling within the scope of the AI Act, and as the market surveillance authority under Article 63, and can even impose fines on EU institutions under Article 72.

On 18 June 2021, the European Data Protection Board ("EDPB") and the Supervisor published their joint opinion No 5/2021 ["EDPS - EDPB Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)"] (hereinafter: the "Opinion") [14] on the draft AI Act. The Opinion welcomed the draft, but called for a number of points to be added. The Opinion disapproves of the exclusion of international law enforcement cooperation from the scope of the draft, as this exclusion poses a significant risk of circumvention, for example by third countries or international organisations operating third party high-risk AIs. The EDPS urges that the concept of 'risk to fundamental rights' be aligned with the GDPR and suggests adding a recital stating that the draft does not intend to affect the application of existing EU legislation on the processing of personal data. In relation to risk assessments, the EDPB and the Supervisor propose that the draft AI Act should be amended so that distributors should carry out an initial risk assessment of the AI, taking into account the use cases, and then the user of the AI should carry out a data protection impact assessment, taking into account the specific context in which the AI will operate. The Opinion calls for a complete ban on "social scoring" and "automated recognition of human characteristics in publicly accessible spaces" without exceptions.

According to the EDPS, national data protection authorities should also be designated as national supervisory authorities for the purposes of Article 59 of the draft AI Act, which would ensure a more harmonised regulatory approach and help avoid inconsistencies between Member States of the EU in the implementation. Finally, the Opinion suggests that national data protection authorities should be involved in the preparation and development of harmonised standards and certificates.

On 28 September 2022, a draft Directive [”Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)”] [15] was published, which mainly addresses civil liability actions in front of a national court, and has no direct data protection implications.

The European Parliament's proposal to the Commission [”European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics”] is also worth mentioning [16]. The proposal deals primarily with robots, i.e. AI with a physical appearance; it has a data protection aspect in that it confirms the application of the principles and methods of the GDPR also to robots. As of February of 2023, the proposal seems to have made no progress.

To sum up, the author concludes that Europe is close to achieving a uniform AI regulation, although it may take some years before this is achieved; at present, however, the EU has only issued formal documents on the subject at a declaratory level. The citizens can find detailed privacy rules in data protection authority’s guidelines, instead of EU mandatory law.

IV. THE CURRENT STATE OF REGULATION IN CHINA

China has taken a number of steps over the last few years to develop data protection and IT regulation. Article 24 of the Personal Information Protection Law of the People's Republic of China (PIPL) [17], in force since 1st of November 2021, dedicated it’s Article 24 to automated decision making. Just like the GDPR, the PIPL dedicates only a small portion to AI. According to the PIPL: „Personal information processors using personal information for automated decision making shall ensure the transparency of the decision making and the fairness and impartiality of the results, and may not apply unreasonable differential treatment to individuals in terms of transaction prices and other transaction conditions. Information push and commercial marketing to individuals based on automated decision making shall be simultaneously accompanied by options not specific to their personal characteristics or with convenient means for individuals to refuse. Where a decision that may have a significant impact on an individual's rights and interests is made through automated decision making, the individual shall have the right to request clarification from the

personal information processor and the right to refuse the processor for making the decision only through automated decision making."

The use of AI appears to be of particular importance in China, with a number of official acts issued in the two years; however, it can be noted that there has been only one binding law, but many more recommendations - three in number - have been issued - although it is presumably worthwhile for stakeholders to follow the recommendations closely.

Not surprisingly, the binding legislation focuses on the sub-area of algorithm-based internet recommendations, as has been the case with the first regulatory instruments in other countries and regions. The legislation, which entered into force from 1st of March 2022 and is jointly subscribed by several governmental bodies (but coordinated by the Cyberspace Administration of China). Although it is called "Internet Information Service Algorithmic Recommendation Management Provisions" [18], we can regard it as binding legislation, since it contains a legal liability section which gives the opportunity to issue warnings, decide about suspensions, or impose fines. The legislation requires algorithm-based internet recommendations to be ethical, moral, accountable and transparent. The regulation requires companies to inform users when an algorithm plays a role in determining what information to display to them and to give users the opportunity to opt out of a targeted recommendation based on their personal characteristics. In addition, the regulation prohibits the use of algorithms that use personal data to offer different prices to different consumers for the same product/service.

Three recent recommendations and guidance documents cover:

1. The "White Paper on Trustworthy Artificial Intelligence" [19] issued by the China Academy of Information and Communications Technology together with JD Explore Academy in July 2021, which, among other things, addresses the privacy challenges of AI systems and recommends avoiding or minimizing the use of personal data where it is not necessary to achieve the purpose of AI. The White Paper's policy recommendations include the creation of trustworthy AI-related legislation in China, the development of commercial AI insurance, and a cautious approach to AI research. The document brings up the example that "the frequent use of biometric authentication increases the risk associated with potential data breaches, which could cause the leaking of confidential user data".

According to the White Paper, "the trustworthy characteristics of AI are summarized by five main aspects: transparency, security, fairness, accountability, and privacy." As we can see, the first four aspects are also connected to privacy.

The White Paper even devotes a separate chapter dedicated to AI privacy protection technologies, analyzing types of attacks against anonymized data sets, and protection approaches like the differential privacy.

2. The "Ethical Norms for the New Generation Artificial Intelligence" [20] issued by the National Governance Committee for the New Generation Artificial Intelligence, which preamble mentions six basic ethical requirements: improving human well-being, promoting fairness and justice, protecting privacy and security, ensuring controllability and credibility, strengthening responsibility, and improving ethical literacy. The third subsection of Article 3 is dedicated to the protection of privacy and security: [AI shall] "fully respect the rights of personal information to know, consent, etc., process personal information in accordance with the principles of legality, justice, necessity, and good faith, protect personal privacy and data security, and must not damage the legitimate rights and interests of personal data, and must not illegally collect and use personal information through theft, tampering, or disclosure information without violating personal privacy."

3. "The Guiding Opinions on Strengthening Overall Governance of Internet Information Service Algorithms" [21], which is the work of several different agencies. This document proposes to strengthen the management control systems of AI programs, and deals with management, regulatory, and supervision issues.

It can be stated that no comprehensive regulation on AI exists in China, but rather separet rules concentrating on specific areas; and a number of guidelines and norms. In an interesting development a comprehensive regulation is already included in the "Municipal Ordinance" of Shenzhen City [Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations] [22]. The city of Shenzhen is important because it was the first so-called special economic zone to be subject to specific rules, and because of this, the zone is home to a number of Chinese technology giants. In addition to supporting R&D projects, the regulation calls for the development of local standards and certification mechanisms, the development of an ethical risk assessment and the establishment of a "Municipal Artificial Intelligence Ethics Committee". The Ethics Committee formulates ethical and security standards; monitors their implementation; analyses the impact of algorithms on the protection of information rights, social ethics, work and employment, etc.; publishes ethical and security practice guidelines, white papers, "good practices"; takes the lead in establishing ethical security management systems for AI.

V. CONCLUSION

The author of the present paper concludes that the need for regulation of AI is a pressing matter. If we see upon the already existing official documents, it is worth contrasting binding regulations with recommendations and guidance documents. Europe is at the forefront of AI regulation, as the GDPR already provides some rules for automated decision-making and profiling, but the draft AI Act and the draft AI Liability Directive are also expected to be adopted in the near future. In the US, there is currently no substantive AI regulation, with changes

expected through ADPPA, which will mandate impact assessments and review of AI systems. In China, binding legislation has only been developed in a sub-area, focusing on algorithm-based internet recommendations; more comprehensive legislation has been developed by the Shenzhen "Municipality" on a territorial basis.

On the other hand, there is a wide range of guidelines, in the EU, guidelines are currently in place rather than comprehensive regulation, see the Council of Europe Guidelines, the European Commission White Paper, the AI HLEG Guidelines. In the US, the Blueprint sets the direction for the development and use of AI, rather than the current lack of binding legislation. In the last two years, China has issued four high-profile official acts on AI, one of which is binding legislation and three recommendations.

In the light of the above, the author of the present paper considers the hypothesis to be well-founded and concludes that there is currently no truly effective, comprehensive and wide-ranging regulation of AI that has already entered into force; and that the current regulation is fragmented, with sub-areas and individual functions being the focus of legislators, and other actors stepping in with unified proposals in this area.

REFERENCES

[1] S.1108 - Algorithmic Accountability Act of 2019, 116th Congress (2019-2020) https://www.congress.gov/bill/116th-congress/senate-bill/1108/text?q=%7B%22search%22%3A%5B%22algorithmic+accountability+act%22%5D%7D&r=2&s=1 [2023. 02. 01.]

[2] S.2968 - Consumer Online Privacy Rights Act, 116th Congress (2019-2020) https://www.congress.gov/bill/116th-congress/senate-bill/2968/text?q=%7B%22search%22%3A%5B%22consumer+online+privacy+rights+act%22%5D%7D&r=1&s=1 [2023. 02. 01.]

[3] H.R.7296 - GOOD AI Act of 2022 https://www.congress.gov/bill/117th-congress/house-bill/7296/actions?s=1&r=2&q=%7B%22search%22%3A%5B%22ai+bill+of+rights%22%5D%7D [2023. 02. 01.]

[4] S.1353 - Advancing American AI Act https://www.congress.gov/bill/117th-congress/senate-bill/1353?s=1&r=4&q=%7B%22search%22%3A%5B%22ai+bill+of+rights%22%5D%7D [2023. 02. 01.]

[5] H.R.8152 - American Data Privacy and Protection Act, 117th Congress (2021-2022) https://www.congress.gov/bill/117th-congress/house-bill/8152/text [2023. 02. 01.]

[6] Office of Science and Technology Policy: Blueprint for an AI Bill of Rights Making Automated Systems Work for the American People https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf [2023. 02. 01.]

[7] 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) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=HU [2023. 02. 01.]

[8] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) https://ec.europa.eu/newsroom/article29/items/612053 [2023. 02. 01.]

[9] Council of Europe: Guidelines on Artificial Intelligence and Data Protection. T-PD (2019)01, Stasbourg, 2019. január 25. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 [2023. 02. 01.]

[10] High-Level Expert Group on AI: Ethics Guidelines for Trustworthy Artificial Intelligence https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai [2023. 02. 01.]

[11] High-Level Expert Group on Artificial Intelligence: Assessment List for Trustworthy Artificial Intelligence https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment [2023. 02. 01.]

[12] WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf [2023. 02. 01.]

[13] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 [2023. 02. 01.]

[14] EDPS - EDPB Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) https://edps.europa.eu/node/7140_en [2023. 02. 01.]

[15] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52022PC0496&from=EN [2023. 02. 01.]

[16] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051 [2023. 02. 01.]

[17] Personal Information Protection Law of the People's Republic of China http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm [2023. 02. 01.]

[18] Internet Information Service Algorithmic Recommendation Management Provisions http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm and https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/ [2023. 02. 01.]

[19] China Academy of Information and Communications Technology together with JD Explore Academy: White Paper on Trustworthy Artificial Intelligence http://www.caict.ac.cn/english/research/whitepapers/202110/P020211014399666967457.pdf [2023. 02. 01.]

[20] National Governance Committee for the New Generation Artificial Intelligence: “Ethical Norms for the New Generation Artificial Intelligence” https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html and https://ai-ethics-and-governance.institute/2021/09/27/the-ethical-norms-for-the-new-generation-artificial-intelligence-china/ [2023. 02. 01.]

[21] Guiding Opinions on Strengthening Overall Governance of Internet Information Service Algorithms http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1779/202109/t20210929_568182.html and https://digichina.stanford.edu/work/translation-guiding-opinions-on-strengthening-overall-governance-of-internet-information-service-algorithms/ [2023. 02. 01.]

[22] Standing Committee of the Seventh Shenzhen Municipal People's Congress: Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations https://law.pkulaw.com/chinalaw/eb370a7e0d9edd5e8ca8bb1a5fa6a5e7bdfb.html [2023. 02. 01.]