ISSN 2029-1701
ISSN 2335-2035 (Online)

Research Journal
PUBLIC SECURITY AND PUBLIC ORDER
2023 (32)

ARTIFICIAL INTELLIGENCE IN FINTECH AND ITS SUSTAINABLE SECURITY NETWORK

Tereza JONÁKOVÁ
Police Academy of the Czech Republic in Prague,
Department of Public Administration
Lhotecká 559/7, 143 00 Prague 4, Czech Republic,
Email: jonakova@polac.cz

DOI: 10.13165/PSPO-23-32-08

Abstract. *Artificial intelligence in relation to the skyrocketing, inter alia, financial technologies brings about a considerable positive potential for humankind in general, none-the-less, along with the clearly associated risks. The impacts of artificial intelligence, Internet of Things and robotics in general have a fundamental impact on public as well as individual security and its guarantees. The financial industry is one of the largest investors in artificial intelligence, with its goal of assuming a primary position in global markets. The conceptual support for artificial intelligence in the scope of its connectivity with the global world against the subtext of its own autonomy, while respecting sustainable development in itself for the future, risk assessment as well as prospective prevention in the area concerned, including lex ferenda, is thus the primary task of a responsible society of the 21st century.*

Keywords: *Artificial Intelligence, Financial Technologies, Responsibility, Security, Sustainability*

Introduction

Artificial Intelligence (hereinafter referred to as "AI"), robotics, and the Internet of Things are integral parts of today's times. Their interconnection alongside their own autonomy, conditioned only by data supplied by man, is a typically finalised product of the human society of the 21st century. AI is a constantly evolving system with a very wide scope of effect and its very existence is demanding due to the complexity of terminological definition and compliance. The European Commission states that: *"AI systems are man-made software and hardware systems that, depending on the intended purpose, operate in a physical or digital dimension, perceiving the environment from data, interpreting structured or unstructured data collected, making causal relationships or processing information derived from that data, and making decisions on the best course of action to be taken to achieve the objective pursued. AI systems can use rules or learn a numerical model, and they can adapt their behaviour by analysing how the environment affects their past actions."*[1] The ability of AI is characterised by imitating human thinking, learning, planning, or creativity, where AI systems are able to work independently and adapt their behaviour based on an evaluation of effects of previous actions.[2] In a way, the cyclical process of AI life learns more the more it performs and gradually leads to "total perfection", engaging in many activities of everyday life. However, the positive benefits are bring along also many pitfalls and threats and it is a challenge for a responsible society to think about the development of AI in the context of adopting responsible limits to its existence.

[1] KOLAŘÍKOVÁ, Linda and Filip HORÁK. *Umělá inteligence & právo*. Praha: Wolters Kluwer, 2020. Legal monograph (Wolters Kluwer ČR). ISBN 978-80-7598-783-9., p. 7

[2] For more detail, cf. *What is artificial intelligence and how is it used?* europarl.europa.eu [online]. European Parliament, 2023, 4. 9. 2020 [cit. 2023-04-04]. Available from: https://www.europarl.europa.eu/news/en/headlines/priorities/artificial-intelligence-in-the-eu/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

In relation to financial technologies (hereinafter referred to as "*FinTech*"), AI represents the current challenge for the future, which is why the financial sector is one of the largest investors in the development and progress of AI. New FinTech technologies based primarily on fast and accurate descriptive big data analytics[3] offer significant innovations in the area concerned, new methods of business models, cost reduction as well as increase in efficiency, all of which is reflected in practical form, for example, in automated trading, creditworthiness assessment, detection of fraudulent actions,[4] in the billing process using the so-called Optical Character Recognition, in the implementation of chatbots/voicebots, innovative hubs, regulatory sandboxes, in the risk management process, etc. In specific areas of FinTech, these include, for example, Blockchain, Cryptocurrencies, WealthTech, InsurTech, RegTech, BigTech, Payments, Banking, Crowdfunding, etc.

The purpose of effective AI networking, also within FinTech, is to sustainably support the interconnection, systematicity, continuity, and creation of effective and efficient cooperation not only of the system itself, but also of its related components within a variable process in terms of the quantity of individual components of networking, as well as their quality. The main objectives of sustainable AI networking can be formulated as follows:

- Support the transformation of the AI system into a sustainable practice / risk identification;
- Strengthen interdepartmental and multidisciplinary cooperation in the development of sustainable AI;
- Establish and support control and supervisory authorities and other key entities in the defined areas of networked AI security and its development;
- Establish and support uniform national and international legal regulations in the field of AI;
- Establish, support, and develop other key entities in the defined areas of networked AI security and its development at the local, national, international level;
- Create, support, and develop tools leading to setting up, identification, and development of quality of key entities in the defined areas of networked AI security and its development;
- Set up and support training modules of key sub-entities in the defined areas of networked AI security and its development.

Secure AI networking in the field of legal regulation

The creation of a secure legal background for AI is a fundamental and paramount task, as AI is considerably faster in its development and the society at the national and international levels is unable to respond adequately to such turbulent pace of development.

The European debate on AI was essentially launched in 2018 and historically includes two key documents - the "Artificial Intelligence for Europe" and the "Coordinated Plan for Artificial Intelligence" from 2018.[5] *"In April 2019, the European Commission followed up with*

[3] For more detail, cf. *Jaký je rozdíl mezi deskriptivní, prediktivní a preskriptivní analýzou?* [online]. [cit. 2023-03-28]. Available from: https://ca-ra.org/cs/jaký-je-rozd%C3%ADl-mezi-deskriptivn%C3%AD-prediktivn%C3%AD-a-preskriptivn%C3%AD-analýzou/

[4] For more detail, cf. *Artificial intelligence: threats and opportunities*. europarl.europa.eu [online]. European Parliament, 2023, 23. 9. 2020 [cit. 2023-04-10]. Available from: https://www.europarl.europa.eu/news/en/headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities

[5] *National AI Strategy of the Czech Republic*. In: . Also available from: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf

the communication 'Building Trust in Human-Centric AI', based on the 'Ethical Guidelines for Ensuring AI Credibility', wherein the High-Level Expert Group on Artificial Intelligence (HLEG AI) listed 7 requirements for trusted AI: human factor and supervision; technical reliability and security; privacy and data protection; transparency; diversity, non-discrimination and justice; good social and environmental conditions and, last but not least, accountability."[6]

At the beginning of 2020, a report on the impact of artificial intelligence, the Internet of Things, and robotics on security and responsibility was published in the White Paper on Artificial Intelligence. In the same year, EU's vision of building trust in AI research was introduced. Following up on the previous documents, in 2021, the European Commission issued the so-called AI package, including a Coordinated Plan on AI and harmonised standards for AI in the internal market.[7]

Over the short history, the significant year for the Czech Republic was 2018, when the Office of the Government of the Czech Republic together with the Technology Agency of the Czech Republic prepared the Analysis of the Development Potential of Artificial Intelligence in the Czech Republic[8] and subsequently the concept of the Digital Economy and Society and the *Innovation Strategy of the Czech Republic* 2019–2030, part of which is also the Coordinated Plan and the National AI Strategy of the Czech Republic.[9]

Due to the wide scope of legislative networking, AI is characterised by an overlap in other legal regulations and disciplines, which may not be primarily an object of interest of AI, but they certainly include it. Specifically, it is necessary to mention AI in connection with the threat of cybercrime. The main legislation is Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA,[10] 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,[11] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of electronic communications data, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013, or Directive (EU) 2022/2555 of the European Parliament and of the

[6] For more detail, see Government of the Czech Republic. *Umělá inteligence* [online]. 06. 12. 2021 [cit. 2023-04-05]. Available from: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/umela_inteligence/umela-inteligence-192765/

[7] For more detail, see Government of the Czech Republic. *Umělá inteligence* [online]. 06. 12. 2021 [cit. 2023-04-10]. Available from: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/umela_inteligence/umela-inteligence-192765/

[8] For more detail, see Government of the Czech Republic. *Umělá inteligence* [online]. 06. 12. 2021 [cit. 2023-04-10]. Available from: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/umela_inteligence/umela-inteligence-192765/

[9] For more detail, see *Národní strategie umělé inteligence v České republice*. In: . Also available from: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf

[10] For more detail, see European Parliament, Council of the European Union. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA in criminal proceedings. 2013. Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32013L0040.

[11] For more detail, cf. European Parliament, Council of the European Union. (2016). 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. Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0679.

Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

In terms of Czech national legislation applicable to AI and FinTech, Act No. 253/2008 Coll., on selected measures against legitimisation of proceeds of crime and financing of terrorism, as amended, should be mentioned. Obligated persons pursuant to the provisions of Section 2 of the aforementioned act include also those who provide services related to virtual assets within cyberspace. Other legislation to be mentioned includes Act No. 181/2014 Coll., on cyber security, as amended, regulating the rights and obligations of individuals as well as powers and competences of public authorities in the field of cyber security. The NIS2 Directive will now impact the area concerned with the requirements to define the basic forms of security measures, to improve the detection of cyber incidents, and to introduce incident reporting along with a system of measures to respond to cyber threats.

Secure AI networking in cyberspace, including the emergence of crime

The term cyberspace first appeared in 1984 in the book Neuromancer by William Gibson, who metaphorically described it as: *"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.* Like city lights, receding…*"*[12] The effort to interpret the concept has been going on for almost 40 years and its definition is still difficult to express, because the scope of cyberspace and its operation are basically intangible. Act No. 181/2014 Coll., on cybersecurity, as amended, understands it as *"a digital environment enabling the creation, processing, and exchange of information, which is formed by information systems and electronic communications networks."*

Due to the diversity of cyberspace in connection with AI and FinTech, significant threats of committing cybercrime[13] and other crimes perpetrated in cyberspace come forward[14]. Asa type of sophisticated crime, cybercrime takes place in the cyberspace environment through modern technologies, anonymously, with a global reach, with remote access, and, in principle, in the short term. In most cases, cybercrimes are very fast and effective, which means that they have the potential to cause extensive damage within a short time, at a relatively low cost. Probably the most prominent specific of cybercrime is the complexity and technical skills that the perpetrators must possess when carrying out primarily cyber-attacks on financial resources and classified information or cyber terrorist attacks.[15]

As part of the classification of types of cybercrime,[16] the Police of the Czech Republic lists fraudulent acts (acts related to fraudulent e-shops, possibly fraudulent advertisements,

[12] GIBSON, William. *Neuromancer*. Translated by Ondřej NEFF. Plzeň: Laser, 1992. Golden sci-fi. ISBN 80-85601-27-3.
[13] Committed in the environment of information and communications technologies, where the main target is the area of IT technologies and their data itself.
[14] General and economic crime committed in cyberspace, where the main object is health, life, morality, or human dignity.
[15]For more detail, see Kaspersky. The Evolution of Cybercrime. [online]. [cit. 2023-03-23]. Available from: https://www.kaspersky.com/resource-center/threats/evolution-of-cybercrime.
[16] For more detail, cf. Police of the Czech Republic. Jednotlivé druhy kyberkriminality [online]. [cit. 2023-03-24]. Available from: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx. Or Podvody v kyberprostoru – Police of the Czech Republic. Úvodní strana – Policie České republiky. [online]. [cit. 2023-02-18]. Available from: https://www.policie.cz/clanek/podvody-v-kyberprostoru.aspx

fundraising, etc.),[17] hacking, blagging, moral crimes (crimes related to the dissemination of child pornography, its production and other use), crimes against copyright (sharing of music, films, and software in violation of copyright), expressing violence and hate crime (dangerous threats, dangerous persecution, spreading of alarm messages).

Secure AI networking in the field of cybersecurity

The policy of secure AI networking from the cybersecurity perspective consists in the overall protection of the participating networks against cyber-attacks and threats. The above can be comprehensively achieved actively responding to negative perceptions and potential threats in the framework of mutual international cooperation and subsequent national coordination.[18] The EU's cybersecurity strategy is to jointly support cybersecurity resilience and the ability to collectively combat cybercrime, which, with a future vision of its sophistication, targets key sectors and critical infrastructure components that are increasingly dependent on digital technologies and their action in the context of AI.

The NIS2 Directive on Network and Information Security aims to respond to the rapidly changing threat environment conditioned by the digital transformation and to ensure a high level of cybersecurity for the EU member states. The Czech Republic will be affected in the planned draft of a new act on cybersecurity in force from the second half of 2024. The Czech Republic presents its attitudes to cybersecurity in the National Cybersecurity Strategy for 2015-2020, and subsequently for 2021-2025[19] with the main task of building and strengthening the cyber defence. The Action Plan on this strategy sees as the responsible entity the Military Intelligence, which is developing the National Cyber Operations Centre for this purpose.

Secure AI networking in the field of supervisory authorities

The supervisory authorities at the national and European levels are characterised by a significant inconsistency, where in the case of one infringement in the form of a cyber-attack (including the participation of AI), the person concerned is obliged to report the incident to several state authorities.

From the position of the European Union, the key supervisory authority is the European Banking Authority (EBA), which oversees the legal regulation of the banking sector, including proposals in the field of crypto-activity, crowdfunding, RegTech, etc.[20,21]

[17] These include, for example, offences endangering the upbringing of a child (Section 201 of Act No. 40/2009 Coll., Criminal Code, as amended, hereinafter referred to as the *"Criminal Code"*), the dissemination of pornography (Section 191 of the Criminal Code), the production and other handling of child pornography (Section 192 of the Criminal Code), the abuse of a child in the production of pornography (Section 193 of the Criminal Code), participation in a pornographic performance or establishing illegal contacts with a child (Section 193b of the Criminal Code), all of the above in addition to new trends such as cybergrooming or cyberbullying. For more detail, cf. Kybergrooming – Prevence kriminality. [online]. [cit. 2023-02-20]. Available from: https://prevencekriminality.cz/kybergrooming/

[18] For more detail, cf. Kybernetická bezpečnost | Government of the Czech Republic. [online]. [cit. 2023-03-20]. Available from: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/

[19] For more detail, cf. Vojenské zpravodajství | Kybernetická obrana. [online]. [cit. 2023-03-21]. Available from: https://vzcr.cz/kyberneticka-obrana-46

[20] For more detail, cf. *Shrnutí výroční zprávy orgánu EBA za rok 2021* [online]. [cit. 2023-03-24]. Available from: https://www.eba.europa.eu/shrnut%C3%AD-výročn%C3%AD-zprávy-orgánu-eba-za-rok-2021

[21] Other European institutions include the *European Securities and Markets Authority* (ESMA) and the *European Insurance and Occupational Pensions Authority* (EIOPA).

To secure cyberspace in the Czech Republic, the National Cyber and Information Security Authority was established in 2017 as the central authority for cybersecurity, including classified information in the field of information and communication systems and cryptographic protection. The National Cyber Security Centre was established as the executive part of the authority, primarily for risk assessment and handling of cyber incidents. The National Security Authority is included in the list of supervisory authorities primarily from its position of cooperation at the international level and education. However, the Action Plan for the National Cybersecurity Strategy identifies the Military Intelligence, the unified intelligence service of the armed forces, as the responsible entity for cybersecurity. In the field of legalisation of proceeds of crime and financing of terrorism, authorities are obliged to report, unlike others, to the Financial Analytical Office.

Secure AI networking in the field of protection of intellectual rights

The Czech legislation does not provide protection for works created by AI, because Act No. 121/2000 Coll., on copyright, as amended, defines the author in the provision of Section 5 (1), where *"the author is a natural person who created the work" and also "works created by independent action of computers or other devices that are capable of self-organization or learning, e.g. in the field of artificial intelligence, are not considered to be the result of creative activity, because they are not the intellectual results of an original creation by a natural person (author)."*[22]

Thus, if AI now creates a "work", the Czech legal order is not ready to apply copyright protection to it and probably the only possible solution is in an amendment to the Copyright Act, which would regulate the protection of AI-related copyright.

The report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the impact of artificial intelligence, the Internet of Things, and robotics on safety and responsibility has raised the issue of the need for consistent regulation, at least regarding the basic rules of operation, not only in relation to the individual interests of individuals, but also within the framework of society-wide systems in which AI is involved and is a common part of the creative process and creation of works. This connection, within any defined author's work, thus establishes a connection with the functional dependence of the "individual" on the AI-generated, which constitute the joint final author's work. The share of liability for damages, including qualified infringement of copyright in the process of creating copyright works, is thus quite obvious, as AI is the co-author of the resulting work. In order to regulate the establishment of liability in relation to AI in the future, it is necessary to unambiguously resolve the method of interference with copyright (i.e., the use of the work, or the handling of the work), the grounds of responsibility for the work (when several authors may participate in the creation of the work itself to varying degrees, with varying degrees of legitimate involvement in the process), and furthermore the liability regime (in principle, predetermining the final form of the original work itself, including the decision to involve AI). The final responsibility can be assumed in the administrative, criminal, and civil spheres (liability in the framework of compensation for damages and the issue of unjust enrichment in the form of financial compensation, satisfaction most often considered in the form of damages from operational activity or damages caused by a thing). Despite the fact that in the case of AI, the general type of liability cannot be applied to all plausible ways of using

[22] For more detail, cf. *Výzkum potenciálu rozvoje umělé inteligence v České republice: Souhrnná zpráva* [online]. 10 December 2018, p. 41. [cit. 2023-03-23]. Available from: https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/AI-souhrnna-zprava-2018.pdf

AI, the most commonly assumed type of AI liability for damage is based on the manufacturer's objective liability, precisely in view of the unpredictability of the actions of autonomously deciding AI systems.

Secure AI networking in the area of responsibility for AI caused damage

Within the automated decision-making processes, AI demonstrates considerable independence on human actions, its own decision-making without the will of a person, thus displaying elements of the application of liability, including causing damage. In connection with the claimed AI authorship of the work, there is also an obvious link to the need to pay attention not only to the appropriate type of liability and responsible "entity", but also to the approach of compensation for damages.

The European Parliament actively addressed the brief history in its reflection from 2020, proposing a civil liability regime for AI, identifying the liability of the objectively responsible operator for the damages caused by AI.[23] At the end of 2022, the European Commission published recommendations for the future regulation of liability for damages caused by AI and liability for damages caused by a product defect. The conclusions of the recommendation showed a clear tendency toward the increased protection of the damaged party in the case of proving the damage caused, establishing the obligation of the AI operator to disclose all data on the operated system, including the introduction of the so-called rebuttable presumption of a causal relationship between the provider's failure to observe due diligence and the damage caused by AI.

In the case of criminal liability, it is based on the fact that AI has no legal personality or free will, therefore, it cannot have legal capacity, whereas any criminal liability is attributed to its manufacturer or programmer.[24] The proposal for compulsory insurance, including the guarantee scheme, has already been discussed in the European Parliament, including Insurance Europe. However, compelling arguments for the general obligation of insurance argue in the opposite that there are not enough representative conclusions about AI and associated risks and that it is not yet possible for one universal insurance for all technologies using AI to exist.[25]

Conclusions

AI constitutes a new phenomenon of the current time with a significant potential to dominate a significant part of human capacities. However, in addition to the obvious benefits that AI exhibits, responsible control of the situation requires the coordination and interconnection of all segments involved in the AI action and the adoption of adequate and appropriate tools for implementation.

In connection with the trend of global trading, AI creates process automation, facilitates the processing of complex problems, and currently becomes established in the field of increasing automation by machine learning, expanding chat bots, developing Quantum AI, integrating AI into IoT, or developing humanoid robots. However, along with very obvious

[23] For more detail, cf. *Změna v odpovědnosti za inteligentní systémy* [online]. [cit. 2023-03-22]. Available from: https://www.epravo.cz/top/clanky/zmena-v-odpovednosti-za-inteligentni-systemy-115449.html
[24] For more detail, cf.: *Justicna revue: Umelá inteligencia a trestná zodpovednosť*? 71. 2019. ISSN 1335-6461., p. 78
[25] For more detail, cf.: *Insurance Europe: Je předčasné zavádět povinné pojištění umělé inteligence* [online]. [cit. 2023-03-24]. Available from: https://www.opojisteni.cz/spektrum/insurance-europe-je-predcasne-zavadet-povinne-pojisteni-umele-inteligence/c:19935/

positives, we are already facing an increased number of constantly improved cyber-attacks against fundamental targets of secure critical infrastructure of high importance, including threats, loss, or misuse of classified data and information,[26] or an increase in new forms of cybercrime.

The challenge for a responsible society of the 21st century using AI consists mainly in sophisticated procedures in relation to the handling of AI, in proper and unified legislation (including joint reflection, for example, on the creation of a completely new subject of rights), supervisory bodies, ethics, moral standards, transparency of safe use of AI, continuous education, and cooperation aimed at prospective fight against cybercrime and abuse of AI.[27]

References

1. Artificial intelligence: threats and opportunities. europarl.europa.eu [online]. European Parliament, 2023, Available from: https://www.europarl.europa.eu/news/en /headlines/society/20200918STO87404/artificial-intelligence-threats-and-opportunities
2. FBI. Cyber Crime [online]. Available from: https://www.fbi.gov/investigate/cyber
3. GIBSON, William. Neuromancer. Translated by Ondřej NEFF. Plzeň: Laser, 1992. Golden sci-fi. ISBN 80-85601-27-3.
4. Government of the Czech Republic. Umělá inteligence [online]. Available from: https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/umela_inteligence/ume-la-inteligence-192765/
5. Insurance Europe: Je předčasné zavádět povinné pojištění umělé inteligence [online].Available from: https://www.opojisteni.cz/spektrum/insurance-eu-rope je-predcasne-zavadet-povinne-pojisteni-umele-inteligence/c:19935/
6. Interpol. Crimes - Cybercrime. [online] Available from: https://www.interpol.int /en/Crimes/Cybercrime
7. Jaký je rozdíl mezi deskriptivní, prediktivní a preskriptivní analýzou? Available from: https://ca-ra.org/cs/jaký-je-rozd%C3%ADl-mezi-deskriptivn%C3%AD-prediktivn%C3 % AD-a-preskriptivn%C3%AD-analýzou/
8. KOLAŘÍKOVÁ, Linda and Filip HORÁK. Umělá inteligence & právo. Praha: Wolters Kluwer, 2020. Legal monograph (Wolters Kluwer ČR). ISBN 978-80-7598-783-9., p. 7
9. Kaspersky. The Evolution of Cybercrime.]. Available from: https://www.kaspersky. com/resource-center/threats/evolution-of-cybercrime.
10. Kybergrooming – Prevence kriminality. Available from: https://prevencekriminality. cz/kybergrooming/
11. Kybernetická bezpečnost | Government of the Czech Republic. [online]. Available from:https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka_bez-pecnost/kyberneticka-bezpecnost-192766/
12. Národní strategie umělé inteligence v České republice. In: . Also available from: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_ 2019.pdf

[26] For more detail, see FBI. Cyber Crime [online]. Available from: https://www.fbi.gov/investigate/cyber [cit. 2023-02-28].

[27] For more detail, cf. Interpol. Crimes - Cybercrime. [online] Available from: https://www.interpol.in t/en/Crimes/Cybercrime [Retrieved on 27.02.2023].

13. Justicna revue: Umelá inteligencia a trestná zodpovednosť? 71. 2019. ISSN 1335-6461., p. 78
14. National AI Strategy of the Czech Republic. In: . Also available from: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf
15. Podvody v kyberprostoru – Police of the Czech Republic. Úvodní strana – Policie České republikyAvailable from: https://www.policie.cz/clanek/podvody-v-kyberprostoru.aspx
16. Police of the Czech Republic. Jednotlivé druhy kyberkriminality [online]. Available from: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.
17. Shrnutí výroční zprávy orgánu EBA za rok 2021 [online]. Available from: https://www.eba.europa.eu/shrnut%C3%AD-výročn%C3%AD-zprávy-orgánu-eba-za-rok-2021
18. Výzkum potenciálu rozvoje umělé inteligence v České republice: Souhrnná zpráva [online]. 10 December 2018, p. 41. Available from: https://www.vlada.cz /assets/evropske-zalezitosti/aktualne/AI-souhrnna-zprava-2018.pdf
19. Vojenské zpravodajství | Kybernetická obrana. [online]. [cit. 2023-03-21]. Available from: https://vzcr.cz/kyberneticka-obrana-46
20. What is artificial intelligence and how is it used? europarl.europa.eu [online]. European Parliament, 2023, 4. 9. 2020. Available from: https://www.europarl.europa.eu/news /en/headlines/priorities/artificial-intelligence-in-the-eu/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used
21. Změna v odpovědnosti za inteligentní systémy [online]. Available from: https://www.epravo.cz/top/clanky/zmena-v-odpovednosti-za-inteligentni-systemy-115449.html

Legislative documents

1. European Parliament, Council of the European Union. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA in criminal proceedings. 2013. Available from: https://eur-lex.europa.eu/legal-content/CS/TXT /?uri=CELEX%3A32013L0040.
2. European Parliament, Council of the European Union. (2016). 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. Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri= CELEX%3A32016R0679.