Studia Bezpieczeństwa Narodowego
Zeszyt 24 (2022)
ISSN 2028-2677, s. 25-46
DOI: 10.37055/sbn/151151

Instytut Bezpieczeństwa i Obronności
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 24 (2022)
ISSN 2028-2677, pp. 25-46
DOI: 10.37055/sbn/151151

Institute of Security and Defense
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

THE APPLICABILITY OF THE GDPR TO ARTIFICIAL INTELLIGENCE AND THE RESULTING THREATS TO NATIONAL INFORMATION SECURITY

STOSOWANIE RODO W ZAKRESIE SZTUCZNEJ INTELIGENCJI I WYNIKAJĄCE Z TEGO ZAGROŻENIA DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA

Tomasz Guta
Akademia Leona Koźmińskiego w Warszawie

Abstract. Both national security and information security are closely associated with and connected to the emerging field of artificial intelligence. In this regard, following the presumed axioms of the anticipated proliferation of AI systems within modern society and its expected widespread implementation in vital public and private institutions and furthermore the extensive application of AI systems within personal data processing, possible threats to national and information security within the European Union - with an emphasis on Poland and the Polish legal system – are explored. On the basis of an overview of the theoretical basis of the concepts of national and information security and artificial intelligence, the emergence of AI within personal data processing in the context of the GDPR legal framework is discussed. At least one potential conflict between the implications of the hypothetical scenario of the emergence of the so-called strong form of artificial intelligence and both the Polish data privacy legal framework (based, inter alia, on the GDPR) and the Polish information security is being identified in this context. The academic article draws the conclusion that the emergence of so-called "strong AI" may lead to a number of real and probable threats to the system of personal data protection and information security in Poland (and possibly in the other EU Member States as well). The paper finally concludes by outlining and discussing the negative impact of the identified conflict, in particular on Polish information security, and calls for efforts to address these issues in future studies in the academic literature.
Keywords: GDPR, A.I., Artificial Intelligence, national security, information security, data privacy

Abstrakt. Zarówno bezpieczeństwo narodowe, jak i bezpieczeństwo informacji są ściśle związane z rozwijającą się współcześnie dziedziną sztucznej inteligencji (SI). W związku z tym, kierując się założonym w pracy aksjomatem oczekiwanego rozprzestrzeniania się systemów SI we współczesnym społeczeństwie oraz ich spodziewanego szerokiego wdrożenia w istotnych instytucjach publicznych i prywatnych, a także szerokiego zastosowania systemów SI w ramach przetwarzania danych osobowych, przeanalizowano w

tejże pracy niektóre możliwe zagrożenia dla bezpieczeństwa narodowego i informacyjnego w Unii Europejskiej - z naciskiem na Polskę i na podstawie Polski i polskiego systemu prawnego. Na podstawie przeglądu teoretycznych podstaw koncepcji bezpieczeństwa narodowego i informacyjnego oraz koncepcji sztucznej inteligencji omówiono w tejże pracy pojawienie się SI w ramach procesów przetwarzania danych osobowych w kontekście ram prawnych RODO. W tym kontekście zidentyfikowany zostanie przynajmniej jeden potencjalny konflikt między implikacjami (hipotetycznego) scenariusza pojawienia się tzw. silnej odmiany sztucznej inteligencji a polskim porządkiem prawnym dotyczącym ochrony danych osobowych (opartym m.in. na RODO) oraz polskim bezpieczeństwem informacji. W tym artykule naukowym sformułowano wniosek, iż pojawienie się tzw. silnej odmiany SI może prowadzić do szeregu prawdopodobnych zagrożeń dla systemu ochrony danych osobowych i bezpieczeństwa informacji w Polsce (a potencjalnie także w innych państwach członkowskich UE). We wnioskach artykułu przedstawiono i omówiono negatywny wpływ wcześniej w nim zidentyfikowanego konfliktu, w szczególności na bezpieczeństwo informacji w Polsce, a także postulowano podjęcie wysiłków w celu rozwiązania tych kwestii w przyszłych rozważaniach i opracowaniach w literaturze naukowej przedmiotu.
Słowa kluczowe: RODO, S.I., Sztuczna Inteligencja, bezpieczeństwo narodowe, bezpieczeństwo informacji, ochrona danych osobowych

Introduction

Artificial intelligence and machine learning techniques are altering the way both private and public organizations gather, process, store, and protect data. One of the challenges of the application of artificial intelligence systems and big data analytics is to maximize utility whilst protecting human and citizen's rights and preserving meaningful human control. In this regard, the main objective of this research paper is to highlight and discuss chosen threats to the information security and the national security of the Republic of Poland – and indirectly to all Member States of the European Union. The issues discussed are raised in the context of the emergence and the widespread application within personal data processing of artificial intelligence systems (and particularly Artificial General Intelligence; AGI) and amid the raised axiom of its anticipated proliferation within modern society and its expected widespread implementation in both public and private institutions. In particular, these issues will be discussed on the basis of the European General Data Privacy Regulation (GDPR) and discussed through the lens of national information security with emphasis on the Republic of Poland and the Polish legal system.

To achieve the outlined aims it will be necessary to (1) briefly present the essence of the currently academically recognized definitions of national security and information security, (2) briefly present the dichotomous division and definition of the phenomenon of artificial intelligence (AI) and (3) by way of a gradual academic examination of the relevant legal norms of the GDPR briefly outline the problems related to the expected manifestation of the strong form of artificial intelligence in the context of the conflict between AI and the GDPR legal framework in its current legal form. Finally, the negative impact of this conflict on national security, and in particular on information security, will be outlined.

The national security and information security of a State. A Polish perspective.

National security in the Polish security studies and legal framework.

To begin the considerations, we need to accurately describe the basic meaning of the crucial terms national security and information security within the Polish national security framework.

In primary European Union law, the concepts of public policy and internal security, as well as national security, appear in Articles 72 and 73 TFEU. However, these provisions do not contain a clear definition of these concepts; rather the EU legislator avoids creating precise regulations and gives them the character of general clauses. Polish constitutional provisions do not contain a legal definition either (Kurek 2021, p. 69). The term national security, it should be stressed, isn't one of a purely legal nature, and furthermore, is a term that is defined by using an interdisciplinary approach. Such an interdisciplinary definition is possible if the definition process takes into account the rich research heritage of the academic field of security studies, which is concerned with an in-depth analysis of the concept of national security (Kurek 2021, p. 53).

Furthermore, the academic doctrine of security studies defines types of state and national security, that are distinguished by the individual values that they protect. Security sciences, therefore, distinguish such security categories as, among others, economic, information, social, political, and military national security. Their scope is limited by the range of values, goals, and interests of the state's security; however, all these categories of state security are contained in the overarching set of national security. Based on one leading scholar's subject analysis „all of them distinguished according to the subject criterion may be perceived as relatively isolated areas of [national] security" (Kitler 2011, p. 40). The predominant view in the doctrine of security studies states that the highest organizational form of a nation that pursues the realization of its national goals is the state that is striving for national security (Haliżak, Popiuk-Rysińska 1995, p. 14).

It is being pointed out that historical experiences from the past, above all related to the tragic experiences of past wars, have led to a narrow political-military understanding of national security due to the predominant and constant imminent threats of armed conflicts (Haliżak, Popiuk-Rysińska 1995, p. 98).

At present, however, this concept has been significantly broadened in security studies to include new dimensions: economic, information, scientific and technical, social, and ecological (Marczak 2008, p. 11). In this academic paper, therefore, a broader definition of the concept of national security is being used.

There is no uniform understanding of this concept in security studies (Kurek 2021, p. 54). W. Kitler defines national security as a process consisting of „various measures in the area of international and internal relations as well as protective and defensive undertakings (in a broad sense) aimed at creating favourable conditions for the functioning of the state in the international and internal arena and at opposing challenges and threats to national security" (Kitler 2011, p. 48).

The author also points out that „the contemporary perception of security is characterized by a departure from the historically fixed beliefs of state security as freedom from external threats and directing more attention to the process of building and maintaining (guaranteeing) the conditions of development, stability, and prosperity of both the state, the whole society and individual citizens, including their tangible and intangible assets and goods" (Kitler 2019, p. 28).

This described evolution in the perception of the substance of the contemporary national security system emphasizes the importance of all the traditional goals of the state in this area but extends its functional scope to a number of social and economic tasks, relevant to the security of individual social groups and each citizen individually (Kitler 2019, p. 28).

P. Tarnoff pointed out, that the 21st century is characterized by the perception of national security through the prism of economics. According to the author, the role of economics in ensuring national security is more vital than the sole military component of security (Tarnoff, Kreisler 1999).

The goal of ensuring favourable conditions for economic and social development [through national security policy] is also indicated by other representatives of American security studies. F.N. Trager and F.N. Simone indicate that it is, to paraphrase their academic argumentation, the goal of state and national security to ensure internal and external conditions conducive to the development of state vital interests and the protection from existing and potential threats (Trager, Simone 1973, p. 61). Furthermore, A. Pūraitė and N. Šilinskė also point out that in the 21st century, the phenomenon of open data, as well as economic and financial aspects, should be regarded as the biggest challenge to the security of European Union citizens after terrorism. According to the authors, this proves the evolution of the security phenomenon at a time when people are looking for a more comfortable life and use more technologies that invade our privacy (such as various aspects of the processing of personal data, CCTV cameras, drones, etc.) (Pūraitė, Šilinskė 2017, p. 137).

In view of the above, a broad concept of national security thus implies the creation of conditions for the well-being of nations and for their unrestricted vital socio-economic development in addition to the bare survival of the state. It includes the combination of two crucial components of national security - ensuring both the survival and the freedom of development of a given entity (Stańczyk 1996, p. 19). Ensuring security is at the same time a dynamic process (conditioned by various external and internal factors e.g., the geopolitical and military situation)

and an object of aspiration to be pursued - an ideal state – a state of safety from threats, which determines the sustainable socio-economic development of the state (Stańczyk 1996, p. 19).

To conclude, therefore, the concept of national security is currently undergoing an important substantive expansion to include new organic dimensions of itself: economic, information, scientific-technical, ideological, cultural, social, and ecological security (Stańczyk 1996, p. 19).

Informational security as part of state national security

The 21st century, known as the information age in literature and culture, has brought about a radical change in the nature and shape of threats to nations and to the world. Related to this is the fact that in times of universal access to information technologies, new dangers closely linked to the use of information networks and information systems emerge (Liderman 2012, p. 24).

The development and widespread use of ICT networks, the general and global availability of electronic devices with access to the Internet, and the widespread use of public networks that transmit information to industrial systems mean that information is also becoming a key factor determining the security of citizens, organizations and entire states (Liderman 2012, pp. 11-12).

Due to the importance of information for today's modern society, the so-called information security, covering all forms of information exchange, storage, and processing, is gaining importance (Liderman 2013, pp. 5).

In this context, an important concept, which is closely interconnected with the concept of „information security" is the concept of the so-called „information society".

The information society has become a conventional term, which illustrates the contemporary social, economic and cultural state of affairs. The foundation of its emergence is the scientific and technological progress lasting since the 20th century, also referred to as the information revolution. (Szempruch 2011, pp. 176-185).

Within the so-defined information society, the continuous existence and development of all entities in this society are possible only by means of universal access to information. That is why we observe the rapid development of technologies enabling its acquisition, transmission, and analysis. Against this background, however, there exists a lack of a clear definition of the term "information society".

In the subject literature, the discussed phenomenon is commonly defined as a society in which information is the key element of both socio-economic activity and changes, and in which technological development makes it possible to generate, collect, process, and transfer information regardless of distance, time and size, which ultimately significantly transforms the way people work and live in a society (Szempruch 2011, pp. 176-185).

Also the concept of the information society, in the opinion of the scientific doctrine, has not yet received an unambiguous interpretation and is used in various meanings, covering all forms of the exchange, storage, and processing of information (Liderman 2012, pp. 13).

According to generally accepted views in security studies, information security concerns an entity (a person or an organisation, including a public organisation) that may be threatened by the loss of information resources or by receiving information of poor quality. Therefore, information security means "the legitimate confidence of an entity in the quality and availability of the information it obtains and uses" (Liderman 2012, p. 22). S. Kowalkowski defines information security as an integral part of national security that accepts the increasing importance of information in maintaining the stability of modern international economic systems and considers the protection against modern threats to and attacks on ITC networks. He ranks informational security alongside economic, political, military, social, cultural, and ecological security (Kowalkowski 2011, pp. 13-15).

This research paper adopts a broad definition of information security, based on the concept developed by E. Nowak and M. Nowak. According to these authors, information security is a state of external and internal conditions allowing a state to freely develop its information society (Nowak, Nowak 2011, p. 103), while as conditions for achieving information security the cited authors assume, inter alia, the following conditions relating to the internal and external spheres of the state:

a) The existence of unthreatened strategic state resources.
b) The principle that decisions by authorities are taken on the basis of reliable, relevant information.
c) The existence of an uninterrupted flow of information between state authorities.
d) The undisturbed functioning of ICT networks forming the critical ICT infrastructure of the state. Crucially, a state's critical infrastructure includes, among other things, the information systems of states and companies (Więcaszek-Kuczyńska 2014, p. 213).
e) The protection of citizens' classified information and personal data [personal data protection] guaranteed by the State.
f) The principle that citizens' right to privacy is not violated by public institutions.
g) Citizens' right to free access to public information.

Finally, complementing this broad definition adopted in this paper, information security is also described in national security literature as a state in which the risk of threats to the proper functioning of information resources is reduced to an acceptable level (Wrzosek 2010, p. 150).

In this respect, threats to information security are associated in the security studies, among others, with the unwanted or unauthorized acquisition, disclosure, modification, or destruction of security-relevant information (security-relevant refers to information affecting the efficient functioning of state structures and society overall) (Polończyk 2013, pp. 2-3) which violates in its effects certain conditions for achieving information security, as proposed by the chosen and used model that defines information security.

Information security is therefore becoming, among other things, a de facto determining force for economic, military and social security, both on a local, national and international level, which is reflected in the information security strategies and government programmes developed and implemented by states, including the Polish state (Więcaszek-Kuczyńska 2014, p. 214).

Types of Artificial Intelligence

The possibility of creating 'thinking' machines raises – among other things - a host of legal issues (see: Kurzweil 1990). In this context, this research paper will present and describe the significant and dichotomous division of artificial intelligence into narrow artificial intelligence (referred to as 'weak' AI or ANI) and general artificial intelligence (referred to as 'strong' AI or AGI). The workings of these two main types of AI will be outlined, on which basis it shall be made clear at what stage of evolution AI currently operates and where the critical distinctions between the two types of AI lie - most notably in the context of the applicability of the GDPR to artificial intelligence entities (AI's).

Intelligence, Artificial Intelligence and Narrow Artificial Intelligence

According to American computer scientist and cognitive scientist John McCarthy, "Intelligence is the computational part of the ability to achieve goals in the world". Varying kinds and degrees of intelligence occur in people, many animals, and some machines" (see: McCarthy 2003). The term Artificial Intelligence (AI) was further famously defined by John McCarthy as "the science and engineering of making intelligent machines". In this context and regarding the most broadly accepted contemporary views in science and philosophy, "intelligence" means "the ability to change the world in order to attain one's goals" (Jebari, Lundborg 2019, p. 1).

Using the European Commission's 2018 definition of AI, "Artificial Intelligence refers to systems that display intelligent behaviour by analysing their environment and taking action – with some degree of autonomy – to achieve specific goals" (Boucher 2020, p. 5). The author of this academic paper subscribes to the EC's fairly generic definition of the concept of artificial intelligence. This definition encompasses the

most essential aspects of the artificial intelligence phenomenon and emphasizes its autonomous nature as an intelligent and independent agent.

Artificial Intelligence can be classified in different ways. If functionality is assumed as the main category for such a classification, three types of artificial intelligence can be distinguished (Perez, Deligianni 2017, p. 6).

The first type of the three basic types of artificial intelligence is Artificial Narrow Intelligence (ANI or "weak AI").

Weak AI or artificial narrow intelligence (ANI) refers to AI systems that operate under a very narrow set of pre-programmed constraints and that can only solve very specifically defined application problems. ANI can only process narrowly defined tasks e.g. facial recognition, speech recognition, searching the internet, and the like (Perez, Deligianni 2017, p. 6).

Narrow AI is inspired by the human brain but does not mimic it. This "soft" type of artificial intelligence merely simulates human intelligence based on a narrow range of parameters, tasks, and contexts. It depends entirely on modern machine learning algorithms which are statistically oriented computational methods for addressing complex problems based on the analysis of vast amounts of information. The results of those methods exhibit qualities we tend to associate with human intelligence (see: Wladawksy-Berger 2016).

ANI is thus "mainly focused on the fulfilment of clearly defined tasks and does not vary its approach to problems" (Hartmann, Allan, Hugenholtz 2020, p. 35). Thus, "weak AI" relies entirely on computational methods – particularly machine learning algorithms – that have been made available to it for problem-solving. Even the most advanced currently available AI system only applies ANI (Hartmann, Allan, Hugenholtz 2020, p. 35).

Examples of "weak AI" include Meta's (formerly Facebook) newsfeed, Apple's Siri virtual assistant, software allowing for autonomously driving cars or facial recognition software.

Artificial Intelligence and Artificial General Intelligence ("strong AI")

It is commonly assumed that AI will ultimately not only become very intelligent but that with the passage of time it will evolve into a conscious agent equipped with so-called general intelligence (i.e., an agent capable of action in many different contexts) (Jebari, Lundborg 2019, p. 1).

Artificial general intelligence (AGI) refers to artificial algorithms that, similarly to the human general intelligence, "(…) can solve a variety of complex problems in a variety of different domains, and that control themselves autonomously, with their own thoughts, worries, feelings, strengths, weaknesses, and predispositions" (Pennachin, Goertzel 2007, p. 1).

These "strong AI" algorithms can therefore exhibit intelligent behaviour regarding both a wide space of problems or goals pursued and a wide array of contexts, in which those problems are encountered and resolved (Boucher 2020, p. 6).

A hypothetical "strong AI" would thus, like a human being, possess self-awareness and be capable of complex intelligent behaviour. It would have the capacity to perceive itself as a sentient agent and therefore "(…) be capable of judgment and decision making, multifaceted problem solving, learning through reading or experience (..) and anticipating" (OECD Digital Outlook Report 2017, p. 298).

"Strong AI", in contrast to "weak AI" would not act reactively, but rather on its own initiative, in an intelligent and flexible way. Currently "strong AI" algorithms do not exist while the most advanced state-of-the-art AI systems are ANI systems.

The emergence of an AGI system would therefore inevitably lead to the materialization of intelligent machines endowed with consciousness and an intelligence that is qualitatively equal to natural human intelligence. Such an emergence would make these intelligent machines effectively equal to humans and would create many legal problems, including within the EU and Polish legal frameworks on data privacy (aspects of which will be described further).

Artificial General Intelligence and Artificial Superintelligence

Artificial Superintelligence (ASI) is a particular form of Artificial General Intelligence. This term refers to an intelligent machine with intelligence far surpassing that of any individual human or any human organization. An intelligent ASI machine surpasses human intelligence across a wide set of skills by several orders of magnitude – that is to say, it would be superintelligent (Jebari, Lundborg 2019, p. 1). The deliberate creation of artificial superintelligence by humans is not possible with current technology and it is unknown whether the development of such an intelligence is even possible.

Interim finding

Even though researchers in the field of AI now agree, that the creation of "strong AI" is merely an engineering problem and technically feasible in principle (Linde, Schweizer 2019, p. 2) only the "weak" form of artificial intelligence exists today. The exact time in the future by which AGI can be realized is not clear. "Weak AI" is only capable of solving very specifically defined application problems. It operates within a very narrow set of pre-programmed constraints and does not vary its approach to problems.

Applicability of the General Data Privacy Regulation (GDPR)

In a basic scenario, in which an intelligent machine equipped with artificial intelligence (an ANI or AGI system) is processing personal data in accordance with Art. 4 Nr. 1 GDPR, the European General Data Privacy Regulation might, in principle, be applicable in such a case (Art. 2 (1) GDPR). This presupposes that the intelligent machine (AI system) processes personal data as a data controller (in accordance with Art. 4 Nr. 1, Nr. 2, Nr. 7 GDPR).

AI-based personal data processing (Article 4 Nr. 1 GDPR)

In order to further this discussion on the subject matter of the paper – the applicability of the GDPR to the various forms of (personal data-processing) AI's and the various resulting implications – it is necessary to explore the meaning of the legal terms "personal data" and "personal data processing" within the context of the EU General Data Protection Regulation.

Regarding the term "personal data", according to the formal legal definition given in Article 4(1) of the GDPR, this term encompasses all information concerning an "identifiable natural person", (the "data subject"). An "identifiable natural person" is a person that can be identified by reference to certain characteristics that comprise that person's identity, such as name, location data, economic qualities, psychological and genetic traits, etc. Regarding the latter mentioned term, Article 4(2) of the GDPR defines 'processing' as any operations that are performed on personal data, including the recording, storing, alteration, use, destruction, etc. by automated or other means (Humerick 2018, p. 402).

The existing forms of artificial intelligence, in general, all consist of the process of machine learning (ML), which itself is based on algorithms that collect, process, and adapt to data from the external world. Artificial intelligence systems, therefore, thrive on a steady supply of data, which to a large degree is constituted of vast amounts of consumer personal data that enable algorithms to expand their knowledge base and to learn. Thus, in order for companies to effectively compete in the current technology-driven marketplace, they collect, store, process, and typically also maintain large sets of consumer personal data (Humerick 2018, p. 395).

It can be thus stated that personal data is a vital and necessary component to the full life cycle of a modern AI system.

Only anonymised data does not constitute personal data and the GDPR does not apply to such type of personal data (Recital 26 of the GDPR).

Therefore, the address or the postcode of an individual, a photograph or an image of a human face, personal financial transactions data of an individual, etc. constitute relevant examples of personal data that are being processed by a large number of data

controllers through their frequent usage of AI and machine learning algorithms on a regular basis (Humerick 2018, p. 395).

In conclusion, insofar as an AI system processes non-anonymised personal data or information – in the sense of Art. 4 No. 2 of the GDPR – that allows for the identification of a specific natural person, directly or indirectly, such AI data processing falls as a matter of principle within the scope of the GDPR.

Furthermore, the AI system used to process personal data must be included among the recipients of Article 4 No. 7 of the GDPR.

Circle of addressees of Article 4(7) GDPR

According to Art. 4(7) GDPR any natural or legal person, public authority, agency, or other body is a "controller", if alone or jointly with others, this entity determines the purposes and means of the processing of personal data.

Intelligent machines equipped with artificial intelligence are therefore in principle not covered by the scope of addressees of Art. 4 (7) GDPR.

According to the current EU legislation and the legislation of all EU member states, for an intelligent machine (AI) to be considered a data controller – according to Art. 4(7) GDPR – a change in the law would be required.

Such a change in the legal framework to allow for a new form of legal personality for intelligent machines or AI would arguably be appropriate regarding "strong AI" systems, which – as stated above in more detail – would be equipped with a human-like consciousness as well as the innate ability to act of its own volition and decide freely as an independent agent. If the AI system reaches such an advanced developmental stage (AGI) the so far existing relevant differences between an intelligent machine and a natural person would vanish so that their legal status – i.a. with regard to EU data protection law – should be aligned with each other (see: EU Parliaments 'Civil law rules on robotics' 2017).

In contrast to the "strong AI" system, there appears to be no sound reason for a similar amendment to the law regarding "weak AI" systems. Such systems by definition have not reached a developmental stage of consciousness, that would in any meaningful way mimic the qualities of the human mind.

Notwithstanding the exclusion of artificial intelligence algorithms from the circle of addressees (the first formal criterion in the here conducted legal examination is not met) the remaining 2 criteria (these are the power over determining both the *means* and the *purposes* of the processing of personal data.) will be analysed in order to evaluate the implications of the emergence of AI technologies on Polish national security in the context of the impact on the data protection legal framework in the EU and in the Republic of Poland.

In the next step of assessing the applicability of the GDPR to AI systems, it is important to moreover distinguish the (prospective) AI data controller from other entities that may fall under the EU/GDPR data privacy legal framework - in particular, the manufacturer of the AI software and the (human) operator of such software (AI).

The determination of the means and the purposes of the processing of personal data

A further criterion for the assessment of the applicability of the GDPR to data processing AI systems is the question of whether the responsible AI system has the appropriate agency. A distinction based on the competency of decision-making regarding the processing of data itself should necessarily be made (see: Directorate D 2010).

According to Art. 4(7) GDPR the determination of a data controller requires such an entity to have the factual power to decide over both the purposes and the means of the processing of personal data. This includes decisions on 'whether', 'why', and 'how' the personal data is processed (see: Directorate D 2010).

Means of data processing

The term "means of processing" relates to "the way in which" a particular outcome or goal is achieved (Art.-29- Gruppe 2010, p. 15). In particular, the specification of an intended data processing procedure, in general, is included by this legal term. This specifically includes a previous specification of a concrete technical framework that includes a defined database structure in conjunction with pre-programmed rules of its own operation (e.g., AI system) (Art.-29- Gruppe 2010, pp. 15-16).

Therefore, based on the definitions set out herein and the wording of the GDPR, the qualification as a data controller (according to Art. 4(7) of the GDPR) requires the concerned entity to effectively have decision-making power over the used means of processing.

If we relate these remarks to artificial intelligence (AI), the AI system could hold the status of a 'controller' if it could autonomously decide about the technical ways in which it processes personal data.

Importantly, a distinction between the controller, the manufacturer of the (AI) software, and the direct human operator (user) of the (AI) software should be drawn at this point. If the manufacturer of the software would pre-program the technical ways of processing personal data in a rigid and unmodifiable way, the AI system could not hold a controller status according to GDPR. In like manner, if the AI software would be pre-programmed in such a way to allow for the direct (human)

user to decide about the specific means of AI personal data processing, the AI system would not hold the decision power regarding the means of personal data processing hence it could not hold the controller status according to Art. 4(7) GDPR.

In principle, since the manufacturer of the AI software builds this software in the first place and furthermore equips it with all technical means required for performing data processing operations, he can be regarded as the default entity that holds the power to decide over the deployed means of processing personal data. Alternatively, if the intrinsic features of the software in question allow the human user of such software to choose between the specific deployed means of data processing, the user himself can be seen as the default entity with the power to decide about the means and the purposes of personal data processing.

The two abovementioned heuristics regarding the default controller – in scenarios of AI deployment for personal data processing – will remain true when "weak AI" is deployed. Artificial narrow intelligence (ANI) systems are "mainly focused on the fulfilment of clearly defined tasks and do not vary its approach to problems" (Hartmann, Allan, Hugenholtz 2020, p. 35). Such systems cannot, in principle, deliberately decide on the specific technical procedures in which they process personal data in order to accomplish goals that have been narrowly defined for them by their manufacturers. Finally, "weak AI" algorithms currently have no power to either exclusively – i.e. excluding other parties such as the manufacturer of the software – access the databases they use or to exclusively manipulate the data contained in those databases. In view of the above, "weak AI" cannot – unlike AGI systems – be classified as having decision-making power over the used means of processing personal data.

Purposes of data processing

One definition of "purpose" according to Art. 4(7) GDPR is "an expected result that is intended or guides the planned actions [of personal data processing]" (Art.-29-Gruppe 2010, p. 15).

With regard to personal data processing performed by intelligent machines (AI), this means that under the GDPR regime and the EU's data protection legal framework their status as a controller would be contingent on whether the AI system is technically and factually both able and competent to intrinsically decide, whether personal data will be processed for a specific purpose chosen independently by the AI system– for instance for AI learning purposes (Machine Learning).

In this context, the manufacturer of the AI should not be authorized to make any specifications regarding the purpose of the data processing. Instead, an independent decision of the AI that is not subject to third-party review as to whether it processes personal data for a specific purpose is required.

The "weak AI" systems are pre-programmed to accomplish very clearly defined tasks in a manner that does not allow them to vary in terms of their approach to solving these predefined problems. Therefore, ANI systems by definition do not have the ability to make autonomous decisions about whether to process personal data in order to pursue a non-predetermined task. By contrast, a "strong AI" system – as outlined above – will decide autonomously what specific personal data it will process in order to accomplish its independently and autonomously chosen concrete task or objective.

All things considered, in the case of the ANI systems ("weak AI") its lack of autonomy over both the means and the purposes of personal data processing (in view of Art. 4(7) GDPR) - notwithstanding its exclusion from the circle of addressees of Art. 4(7) GDPR and its lack of legal personhood - has the effect that only the manufacturer of the AI software or alternatively the human operator of the AI software may potentially hold the legal status of a data controller (GDPR) and thus be subjected to all the associated controller obligations that are included in and regulated by the GDPR legal framework. As far as the AGI („strong AI") system is concerned, should it be conceived and employed in the processing of personal data, it would meet all the cardinal requirements of Art. 4 (7) GDPR.

The exclusion of AI systems from the legally defined group of addressed entities of article Art. 4 (7) GDPR does not, however, allow it to be qualified as a controller under the GDPR legal regime.

The legal status of AI under the GDPR and prospective implications for national security.

Current legal status of AI under the GDPR regime and additional observations

It should be noted that there are three forms of AI ("weak AI", "strong AI" and "superintelligence"). It must be further noted, that according to the current developmental status of intelligent machines, only "weak AI" systems are being implemented and used in practice. Since, as formerly stated, Artificial Narrow Intelligence systems ("weak AI") have no factual power to decide over neither the means nor the purposes of the processing of personal data, they currently – similarly to hypothetical AGI ("strong AI") systems – do not and cannot hold the status of a data controller under the GDPR regime.

The issue discussed becomes troublesome and problematic when AI systems will become as intelligent as the human beings who initially created them. With the emergence of Artificial General Intelligence (so-called "strong AI") systems, as pointed

out in the preceding discussion, it would have to be considered whether such AI systems are equivalent to natural persons in terms of data protection law – and other areas of law, accordingly considering their legal personhood from a holistic point of view – and whether they can be considered under the GDPR as data controllers that are subjected to all associated controller obligations as regulated by the GDPR.

Legal implications for national security

The conclusions reached so far on the issues of artificial intelligence systems and national security as described here, of course, also have implications in the context of threats to information security and national security.

Taking into account the broad concept of information security developed by E. Nowak and M. Nowak and discussed previously, the emergence of strong AI may lead to a number of realistic and probable threats to the system of personal data protection in Poland (and other European states), and consequently to information security and national security in Poland.

In the opinion of researchers from the field of security studies, the uncontrolled development of bioinformatics technologies – and „strong AI" would naturally fit such a categorization – can lead in the future to the emergence of new threats, also to threats in the area of information security. These threats may eventually prove to be much more serious than those currently identified and lead to a conflict between neuroinformatics engineering inventions with the existing ethical and moral systems – artificial intelligence research in particular provides an excellent example of this trend (Więcaszek-Kuczyńska 2014, p. 222).

In view of the possible emergence of the phenomenon of the so-called „strong AI" as discussed in this paper, threats to a number of prerequisite conditions (or principles) that ensure the information society – as outlined in the aforementioned model by E. Nowak and M. Nowak – are emerging. Here we shall focus on and discuss one main prerequisite condition, that most certainly would be at high risk – namely the condition of "the protection of citizens' classified information and personal data guaranteed by the State" (other prerequisite conditions to information security might also be at high risk).

Condition of the protection of citizens' classified information and personal data guaranteed by the State

Strong AI – if it were to emerge – lacks, according to the current state of legislation in Poland and other European jurisdictions, legal personhood and therefore cannot have the status of a GDPR data controller. It would, however, be equipped with the inherent ability to make autonomous decisions regarding personal data that could be processed by it and the specific purposes it wishes to achieve through such processing activities.

An outline of some of the apparent and unresolvable conflicts and contradictions that arise from the introduction of an emerging "strong AI" operating as the de facto controller of personal data will be given at this point in this work. The author wishes to identify and highlight some of the flagrant breaches of the data protection law system that would likely arise with the introduction of „strong AI" systems to personal data processing and administration. It is not the author's intention to present the full spectrum of such conflicts. A further and more comprehensive description of these challenging issues, including possible solutions at the legal and non-legal levels, is left for future discussions in the literature.

Personal data protection is a relatively new field of law in the Polish legal system. Its introduction results from the adoption of numerous international agreements and treaties on human rights and data privacy, including in particular the GDPR (Depo, Mazur 2015, pp. 90-91). The processing of personal data shall mean any operation performed upon personal data (such as collection, storage, alteration, disclosure, and erasure; and in particular those performed within IT systems).

The GDPR in its Article 5 positively defines principles relating to the processing of personal data, particularly including the following principles:

- „lawfulness, fairness, and transparency",
- "purpose limitation",
- „data minimisation",
- „accuracy" and
- "integrity and confidentiality" of data personal processing.

On the basis of these principles, the views of Polish legal scholars (legal doctrine) formulate a non-exhaustive set of core principles guaranteeing personal data protection (as described earlier in this paper).

We can then confront these principles with the hypothetical operation of a „strong AI" system that is processing and manipulating personal data in an autonomous manner in the information security-relevant systems of public and private organizations. Its actual role as a personal data administrator would not justify – in line with what has been established earlier – the legal status of a controller (GDPR) of such a system.

The principle of lawfulness imposes on the controller and processor the obligation to prove at least one of the prerequisites for the legitimacy of the processing of personal data, in particular the consent of the data subject (Depo, Mazur 2015, p. 97). A hypothetical artificial intelligence system of the AGI type has a mind similar in its nature to a human being and is endowed with decision-making autonomy. Therefore, in principle, it is not possible to force nor even effectively control such a system as regards its decisions on the means and purposes of personal data processing. The system, completely independent of its creator (software manufacturer) and in practice unconstrained by the rules of handling personal data as specified in its source code or in the applicable laws that restrict the GDPR data controller,

can make such decisions completely independently. This state of affairs in effect disrupts the upholding of the principle of legality.

The same applies to the principles of the so-called purpose-specification and the so-called adequacy, which in practice mean that the data controller is not allowed to omit or conceal the purpose of data collection from the data subject and, furthermore, that the data controller should process only the type of data and only the content of data which is necessary for the purpose of data collection (Depo, Mazur 2015, pp. 98-99). An AI system with full autonomy and power over the means and the purposes of personal data processing will not inherently be bound by the GDPR data controller obligations described in these two principles. In particular, such a divergence from the standards of both these principles may necessarily take place within the processes of machine learning (ML) and deep learning, in which the AI system acquires massive amounts of data (e.g., personal data) for the purpose of an autonomous and unassisted learning process based on state-of-the-art neural networks (models). As the sheer quantity of data is positively correlated with the quality of the AI's learning process, the legislatively required discrimination of data will de facto not occur in the process of data acquisition for ML purposes. Consequently, the hypothetical „strong AI" system that would operate as a (personal) data administrator would disrupt both aforementioned principles.

Finally, the principle of substantive correctness, which requires the data controller to ensure the substantive correctness of processed personal data, means in practice that the data are to be truthful, complete, and up to date. However, a hypothetical „strong AI" system equipped with full autonomy and power over the means and the purposes of personal data processing will operate under the constant pressure of having to perform data-intensive machine learning processes to achieve its self--selected goals. Such an AGI system, operating in the competitive framework of other such goal-oriented autonomous AI systems, while performing machine learning activities, will primarily focus on the high volume of collected data in order to increase the likelihood of achieving its stated goals. Although the substantive correctness of the collected data is important in the context of machine learning objectives, it must be assumed that such a system will not optimize its operation to ensure the substantive correctness of personal data, especially in a scenario of conflict with other objectives that this autonomous system will inherently simultaneously pursue.

Ensuring the implementation of personal data protection in the absence of a responsible party

Finally, we should ask whether the condition of the "protection of citizens' personal data", which is guaranteed by the State (as described in the legal theoretical model by the authors E. Nowak and M. Nowak shown earlier), is not violated due to the lack of a legally responsible entity in this area.

According to Article 5(2) GDPR "the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')". It is therefore the (GDPR) data controller that is responsible – either in part or in whole – for complying with Article 5(1) of the GDPR, in addition to its other obligations arising explicitly from the GDPR, which are also imposed on him solely or jointly with other actors within the data protection system (see: Directorate D 2010; Opinion 1/20 of the European Commission the outlines a number of exclusive responsibilities of the controller).

The result of the analysis undertaken in section 3.3 of this work points to the legal inability of 'strong AI' systems to hold the legal status of a GDPR data controller. According to Art. 4(7) GDPR the determination of a data controller requires such an entity to have the factual power to decide over both the purposes and the means of the processing of personal data. However, the AGI system in such cases is the sole entity – as opposed to the manufacturer of the software or the operator of the system – that can effectively be considered the controller of the personal data (see comments above).

Due to this conflict between the factual situation and legal situation in case of the emergence of "strong AI" systems, there is no de facto and de jure entity guaranteeing the implementation of the principles set out in Article 5(1) GDPR. This state of affairs would directly prevent the fulfilment of the state's guarantee of the protection of personal data and would therefore undermine the state's information security.

Altogether, it can therefore be noted that the emergence of AGI systems and their deployment as de facto personal data administrators would cause a direct and irresolvable conflict with some of the above-mentioned, overarching principles of the GDPR (see Article 5 GDPR). The emergence of a so-called "strong AI", therefore, leads to a number of direct threats to the data protection regime in Poland (and indeed, presumably also within other member states of the European Union) and, consequently, to information security and national security in Poland.

Conclusions

It should be noted that there are three main types of artificial intelligence (so--called artificial narrow intelligence or "weak AI", artificial general intelligence or "strong AI" and artificial superintelligence or "superintelligence"), although according to the current state of technological development only "weak AI" systems are being used in practice.

We can further observe that for as long as only „weak AI" systems exist and are being applied to personal data processing tasks, the EU data protection regulations (especially the GDPR) in all probability are sufficient to effectively protect the

GDPR legal standards in the context of a widespread application of ("weak") AI to data processing within the EU and Poland. In such cases, in all probability, either the (human) operator or alternatively the manufacturer of the AI software will be deemed a data controller (GDPR) – with all associated obligations that result from this status.

The situation under discussion becomes very problematic in the event that AI's reach the level of becoming effectively as intelligent as humans. In that case, there exists a conflict – as described above – between the GDPR legal framework (and simultaneously the information security of both Poland and EU Member States) and the factual situation in which an intelligent entity without the legal status of a GDPR controller and without the associated controller obligations towards GDPR data subjects will de facto have full control over the means and purposes of data processing. This state of affairs furthermore poses a significant risk to the Polish and European data privacy legal systems and the information security of all EU Member States.

Provided that the technical developments reach the level of a so-called „strong AI" system, which is comparable to a human being in terms of intelligence, it would have to be considered whether such a system is equivalent to a natural person in terms of the European and Polish data protection legal system and whether it qualifies as a data controller under the GDPR legal regime.

According to the current legal situation within the European and the Polish data privacy law, this requires a legislative amendment, for an intelligent machine, and thus AI, to be considered a data controller.

To ensure a frictionless coexistence with artificial intelligence in the future, it would make sense to enact a robot law (e.g. RobotAct) that contains basic principles governing artificial intelligence and that ensures that humanity is not displaced by intelligent robots. The proposal for a regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence ("Artificial Intelligence Act") clearly appears to be the first major step in this respect.

All problems identified in this paper that arise from the emergence of „strong AI" in the context of both the European and Polish data protection legal systems and within both the Polish and European national information security, justify, in the opinion of the Author of this paper, the need for further efforts to address these problems in future studies in the academic literature.

BIBLIOGRAPHY

[1] Art.-29- Gruppe, 2010, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, Working Paper 169.

[2] Boucher, P., 2020, Artificial intelligence: how does it work, why does it matter, and what we can do about it?, European Parliament, Directorate-General for Parliamentary Research Services, European Parliament.

[3] EU Parliament, 2017, Civil law rules on robotics, European Parliament, http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_ENG.html (Date of access: 2.1.2022).

[4] Depo, J., Mazur, S., 2015, Administracja bezpieczeństwa, informacji niejawnych i danych osobowych, Kraków, Vademecum, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Wydział Nauk o Bezpieczeństwie.

[5] Directorate D (Fundamental Rights and Citizenship) of the European Commission, Directorate-General Justice, 2010, Opinion 1/2010 on the concepts of „controller” and „processor, Brussels, Freedom and Security.

[6] Haliżak, E., Popiuk-Rysińska, J., 1995, Państwo we współczesnych stosunkach międzynarodowych, Warszawa, Wydawnictwo “Scholar”

[7] Hartmann, C., Allan, J., Hugenholtz, P., et al., 2020, Trends and developments in artificial intelligence: challenges to the intellectual property rights framework: final report, European Commission, Directorate-General for Communications Networks, Content and Technology, Brussels, https://data.europa.eu/doi/10.2759/683128 [Accessed 12 February 2022].

[8] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019, Brussels, European Commission.

[9] Humerick, M., 2018, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, Santa Clara, Santa Clara High Tech. L.J. (393).

[10] Jakubczak, R., 2008, Podstawy bezpieczeństwa narodowego Polski w erze globalizacji, Warszawa, Wydawnictwo Akademii Obrony Narodowej.

[11] Jakubczak, R., 2004, Obrona narodowa w tworzeniu bezpieczeństwa III RP, Warszawa, Dom Wydawniczy Ballona.

[12] Jebari, K. and Lundborg, J., 2021, Artificial superintelligence and its limits: why AlphaZero cannot become a general agent, AI & SOCIETY, Vol. 3/2021.

[13] Kesa A. and Kerikmäe T., 2020, Artificial Intelligence and the GDPR: Inevitable Nemeses?, TalTech Journal of European Studies, Vol.10 (Issue 3).

[14] Kurek, J., 2021, Bezpieczeństwo Państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big data. Aspekty prawne, organizacyjne i systemowe, War Studies University.

[15] Kitler, W., 2011, Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system, Warszawa, Akademia Obrony Narodowej.

[16] Kitler, W., 2019, System bezpieczeństwa narodowego RP – aspekty prawno-organizacyjne, Warszawa, Wiedza Obronna, t. 268 nr 3.

[17] Kowalkowski, S., 2011, Niemilitarne zagrożenia bezpieczeństwa publicznego, Warszawa AON.

[18] Kurzweil, R., 1990, The age of intelligent machines. Cambridge, Mass, MIT Press.

[19] Liderman, K., 2012, Bezpieczeństwo informacyjne, Warszawa, Wydawnictwo Naukowe PWN.

[20] Liderman, K., Malik, A., 2013, Polityka informacyjna a bezpieczeństwo informacyjne, Warszawa.

[21] Linde, H., Schweizer, I., 2019, A White Paper on the Future of Artificial Intelligence, Boston, MIT Press.

[22] Marczak J., 2008, Bezpieczeństwo narodowe – pojęcie, charakter, uwarunkowania, Warszawa, [in:] R. Jakubczak, J. Marczak, K. Gąsiorek, W. Jakubczak, Podstawy bezpieczeństwa narodowego Polski w erze globalizacji.

[23] McCarthy, J., 2003, What is artificial intelligence?, At http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html, [accessed 04 January 2022].

[24] Nowak, E., Nowak, M., 2011, Zarys teorii bezpieczeństwa narodowego, Warszawa, Difin SA.

[25] OECD Digital Economy Outlook, 2017, Paris, OECD Publishing.

[26] Pennachin, C., Goertzel, B., 2007, Contemporary Approaches to Artificial General Intelligence, In: Goertzel, B., Pennachin, C. (eds) Artificial General Intelligence. Cognitive Technologies, Berlin/Heidelberg, Springer Verlag.

[27] Perez, J. A., Deligianni, F., Ravi, D., Yang, G., 2017, Artificial Intelligence and Robotics, London, EPSRC UK-RAS Network.

[28] Polończyk, A., 2013, Zagrożenia bezpieczeństwa informacyjnego na przykładzie Krajowej Mapy Zagrożeń Bezpieczeństwa, Kraków, Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej, Instytut Bezpieczeństwa i Edukacji Obywatelskiej.

[29] Puraite, A., Silinske, N., 2017, Understanding the concept of security: theoretical approach, Public Security and Public Order, Vol. 19, pp. 135-145.

[30] Szempruch, J., 2012, Nauczyciel w warunkach zmiany społecznej i edukacyjnej, Kraków, Oficyna Wydawnicza Impuls.

[31] Stańczyk, J., 1996, Współczesne pojmowanie bezpieczeństwa, Warszawa, Instytut Studiów Politycznych Polskiej Akademii Nauk.

[32] Tarnoff, P. Kreisler, H., 1999, Making Foreign Policy in a Democracy: Conversations with Peter Tarnoff, In Conversations with History Series, Berkeley (CA), Institute of International Studies, http://globetrotter.berkeley.edu/people/Tarnoff/tarnoff-con0.html., [Accessed: 22.02.2022].

[33] Trager F.N., Simone F.N., National Security and American Society, 1973, Wrocław [in:] Leksykon politologii, cited after: R. Jakubczak (red.), 2004, Obrona narodowa w tworzeniu bezpieczeństwa III RP, Warszawa.

[34] Więcaszek-Kuczyńska, L., 2014, Zagrożenia bezpieczeństwa informacyjnego, Warszawa, Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej.

[35] Wladawksy-Berger, I., Soft' Artificial Intelligence Is Suddenly Everywhere, January 16, 2016, The Wall Street Journal, http://blogs.wsj.com/ cio/2015/01/16/soft-artificial-intelligence-is-suddenly-everywhere/, [Accessed: 18.02.2022].

[36] Wrzosek, M., 2010, Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną, Warszawa, AON.

LEGAL ACTS

[1] Constitution of the Republic of Poland No. 483 of 2 April 1997.

[2] Treaty on the Functioning of the European Union, Consolidated Text "Official Journal of the European Union', 26.10.2012, C 326.

[3] 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).