DOI: 10.13166/WSGE//VPTV1229

*Greta Angjeli*
*gretaangjeli@umsh.edu.al*
*ORCID ID: 0000-0003-1705-3355*
*Besmir Premalaj*
*besmir.premalaj@umsh.edu.al*
*ORCID ID: 0000-0002-5737-8325*
Mediterranean University of Albania

# THE RIGHT TO RESPECT PRIVATE LIFE IN THE CONTEXT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE

## Abstract

One of the fundamental human rights protected by various international conventions is the right to the protection of privacy, or as defined in the European Convention on Human Rights, the right to respect private and family life. Affiliated to this right is also the right to data protection, which is described by various authors as a modern derivation of the right to privacy protection. The protection of personal data in the context of privacy protection was jeopardized by the rapid and widespread of information technology, automated data processing and the risk of access to this data by unauthorized persons on the network. The legal regulation for the non-violation of the right to respect private life by the processing of personal data with automated systems was one of the challenges of many states which had to allow the use of artificial intelligence for the benefit of further economic and social development, at the same time they had to ensure the protection of the personal data of their citizens. In this context, the EU has issued another regulation on personal data protection (General Data Protection Regulation (EU) 2016/679). The purpose of this paper is to highlight the impact of artificial intelligence on the right to respect private life and the legal protection of personal data from misuse through artificial intelligence.

**Keywords:** *right to respect private and family life, right to data protection, artificial intelligence.*

## Definition of Artificial Intelligence

Since the creation of the first automated systems, it has been alluded to whether there is any form of artificial intelligence. Especially with the creation of integrated circuits, many computer programs associated with the right hardware manage to perform calculations that a person needs a very long period to perform. In some cases, the capabilities of computer systems have even surpassed human capabilities. Some have defined these achievements under the term artificial intelligence. Others are of the opinion that something created by man cannot exceed his abilities. However, many automated systems have already become autonomous. Their autonomy has fueled people's perception of the existence of an artificial intelligence.

There are several definitions of artificial intelligence. Computer science researchers distinguish between four possible approaches. A computer program can be described as intelligent if it:

1. behaves like a human
2. thinks like a human
3. think rationally
4. behave rationally.

According to a first approach, a computer program is intelligent if it **behaves like a human**. One of the tests that proves the intelligence of a computer is the Turing test. According to this test a human asks a computer questions. The received answers will be partly written by a human and partly by the computer. If the computer's answers can no longer be distinguished from the human answers, the test is passed, and the computer program can be classified as intelligent[1]. But because of the successive development of technology the Turing test does not appear to be very effective in many contexts. For example, since the use of computer programs in self-driving cars and other automated processes, it can´t be told that a self-driving car is intelligent and it cannot be distinguished from a man. Something different applies to the phenomenon of social bots, which are specifically designed to simulate human behavior. This are for example certain forms of interaction, like expressions on the Internet such as tweets, posts, likes, comments, etc. According to this first approach,

[1] Russell/Norvig, Artificial Intelligence. A Modern Approach, 2010, p 2.

computer programs can also be classified as intelligent beyond the Turing test, the behavior of which can no longer be distinguished from human behavior[2].

A second approach is based on whether a computer program **thinks like a human** when overcoming problems[3]. It's obvious that the characteristics of human thinking, because of its complexity, cannot be completely imitated by the computer. It will be therefore more reasonable to approach the opinion that a computer is intelligent, if he exhibits certain characteristics of human thinking. The first concept of artificial intelligence, that sustains this second approach, was defined by John McCarthy in 1956. According to him artificial intelligence is the ability of computers to learn that enables them to process more difficult tasks–from playing chess to language and image recognition to translation[4]. Computers that are intelligent can improve their skills not based on a fixed program, but through training and experience and this makes them similar to humans.[5] If artificial intelligence will be defined as an adaptive system, then their use in the digital space has an impact on opinion-forming, for example when sorting search results through Google or sorting news through the Facebook newsfeed[6].

According to a third approach, intelligent systems are characterized by the fact that they **think rationally**[7]. In this point Intelligence is equated with logic. However, this understanding is only useful where facts can be expressed in logical notation[8].

The fourth approach understands under artificial intelligence that computer programs **behave rationally**[9] or that they **produce intelligent results**[10]. This definition seems to be the most avowed in the public debate. Although there are objections to this definition because the solution to any more complex problem, which traditionally could not be solved by computer programs, can be described as intelligent[11]. Some authors describe artificial intelligence as

---

2 Unger/Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, p 5.
3 Russell/Norvig, Artificial Intelligence. A Modern Approach, 2010, p 3.
4 Eberl, Aus Politik Und Zeitgeschichte 6–8/2018, p 8 (9).
5 Russell/Norvig, Artificial Intelligence. A Modern Approach, 2010, p 86.
6 Unger/Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, p 6.
7 Russell/Norvig, Artificial Intelligence. A Modern Approach, 2010, p 4.
8 Unger/Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, p 6.
9 Russell/Norvig, Artificial Intelligence. A Modern Approach, 2010, p 4.
10 Surden, Concurring Opinions, 2012, https://samirchopra.com/2012/01/31/concurring-opinions-online-symposium-for-a-legal-theory-for-autonomous-artificial-agents/ <04.06.2021>.
11 Unger/Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, p 6.

intelligent agents that can "operate autonomously, observe their environment, exist over a longer period, adapt to changes and define and pursue goals. A rational agent acts in such a way that he achieves the best result or the best expected result"[12]. Autonomous operations not only includes physically embedded agents such as autonomous vehicles or service robots, but also computer programs such as the sorting algorithms from Google or Facebook[13].

Artificial Intelligence as physically non-embedded programs are typically characterized by the processing of huge amounts of data and their ability to learn. Orientation in a space and robotics are irrelevant in such a case. This is typical for physically embedded agents. The sorting algorithms of Google and Facebook instead process huge data records on websites or user behavior in order to be able to display the appropriate pages to their users in a meaningful order. There are two relevant criteria to define computer programs as intelligent: the presumed interest of the user as a criterion for priority ads and the presence of offensive content as a criterion for suppressing an ad. Learning methods are used in this direction to make the sorting algorithm interesting or recognize offensive websites[14]. "Learning" means that an algorithm analyzes data, recognizes patterns and develops and refines models, for example to determine user interest or the objectionability of a website. This determination is mostly based on statistical probabilities[15].

The last-mentioned definition of artificial intelligence (intelligence as an intelligent result) especially the development of Google and Facebook algorithms, but not only these, bring risks related to respect the right to privacy and for data protection in this context. But also other definitions of artificial intelligence may also violate the right to privacy.

[12] Russell/Norvig, Artificial Intelligence. A Modern Approach, 2010, p 4.
[13] Unger/Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, p 6.
[14] Unger/Ungern-Sternberg, Demokratie und künstliche Intelligenz, 2019, p 7.
[15] Russell/Norvig, Artificial Intelligence. A Modern Approach, 2010, p 693.

## The right to private life and data protection

The interaction of artificial intelligence with social life increases the risk of exposing a person's private life to the public. Various programs, an integral part of artificial intelligence, having access to our personal data, including photos and statistical data about our behavior, increases the risk of violating one of the fundamental human rights, the right to privacy, sanctioned in Article 8 of the European Convention on Human Rights. While in the European Convention on Human Rights the right to data protection is protected by Article 8 of this convention, other international agreements qualify the right to data protection as a separate right. Thus, for example Eu Charter distinguishes between the right to respect for private life and the protection of personal data (Articles 7 and 8 of the Charter). Yet both rights have the same object of protection, the private life of the individual, his autonomy and his dignity by granting him a personal sphere in which he can freely develop his personalities. Guaranteeing the right to privacy and data protection ensures the free exercise of other human rights, such as the freedom of thought, conscience and religion (Article 10 of the Charter), freedom of expression and information (Article 11 of the Charter), and freedom of assembly and of association (Article 12 of the Charter)[16]. For this reason, in many cases the right to protect private life have been described as a classic right, while the right to personal data protection as a modern right[17].

The concept of privacy is very broad and touches some aspects of a person's physical and social integrity. Giving an exhaustive definition of the term "private life" is difficult and involves several fields of science, not only psycho-social sciences but also law and beyond. This should include the physical and psychosocial aspects of the person. Also defining the boundary of a person's privacy in a public place is a challenge. The European Court of Human Rights (EctHR) has provided a definition of the concept of "reasonable expectation of privacy" in relation to the privacy of individuals in public places[18]. The point

[16] FRA, Council of Europe and EDPS (2018), Handbook on European data protection law. 2018 Edition, Luxembourg, Publications Office, June 2018, p. 19.

[17] CJEU, Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke and Eifert GbR and Hartmut Eifert, Opinion of Advocate General Sharpston, 17 June 2010, para. 71.

[18] Vermeulen, M. (2015), SURVEILLE Deliverable D4.7 – The scope of the right to private life in public places, July 2014, p. 2.

of view in which the EctHR has assessed this aspect, is the fact how much privacy a person can expect when he is in a public place. So factual situations affect the reduction of a person's privacy.

Also exposing a person to the public relativizes his privacy. We cannot expect the same level of privacy for a person who is a public figure and a person who has withdrawn from public life. In this case we have a competition of the right to information and the right to privacy. However, the UN Human Rights Committee notes that even public figures cannot be deprived of their privacy[19]. Restricting their privacy should be proportionate. Like all human rights, the right to data protection is not absolute. It may be subject to restriction in favor of public interest.

Extensive use of artificial intelligence can greatly restrict a person's privacy and their right to privacy. Building a series of algorithms not only in social networks, but in all areas related to network communication and automated data processing, can seriously violate the right to privacy. Different algorithmic mechanisms can process information about a person's behavior and build an initially social profile, but with a more in-depth processing of data also a psycho-social profile of a person. The person navigating the web is not aware of sharing his data with third parties. Often the use of these algorithms is justified by improving customer service and facilitating the retrieval of information that is relevant to the customer. But then the data collected was used for targeted advertising[20]. Everything is justified by the fact of improving customer service and making it easier to find things he is interested in. Also uncontrolled provision of data on the network can expose the person to manipulation, fraud, discrimination, etc.

Although the right to privacy may be violated by the extended application of artificial intelligence, the use of artificial intelligence has the greatest impact on the right to data protection. In this aspect the EU implemented a new regulation, the Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), which repealed the Directive 95/46 / EC. The entered into force in 2016, but began to apply

[19] UN, Human Rights Committee, General Comment No. 37 (2020) on the right of peaceful assembly (article 21), CCPR/C/GC/37, 17 September 2020, para. 62.

[20] FRA, Getting the future right – Artificial intelligence and fundamental rights. 2020 Edition, Luxembourg, Publications Office, 2020, p. 61.

starting from 25 May 2018. It applies both in cases of data processing within the EU, as well as in case the data are processed outside the EU, but the persons whose data are processed are located within the EU. The GDPR applies also in cases where the legal entity that processes this data is headquartered in the EU[21]. However, this regulation applies only to identified or identifiable natural persons[22]. A person is identified, when with the collected data he can be immediately identified. On the other hand a person is identifiable if even only indirectly, for example by obtaining additional data, can be concluded in that person[23].

Responsible for the implementation and observance of the provisions of the GDPR is the natural or legal person who decides on the purpose and means by which the processing of personal data will be performed. This person has a burden of proof if a personal data breach is alleged during the collection or processing of data[24]. The GDPR is guided by general principles of data protection and does not explicitly provide rules relating to the use of algorithms or artificial intelligence in general. Only in some cases are special rules mentioned for Profiling or for automated decisions[25]. The principles by which the GDPR is governed are the principles of lawfulness, fairness, transparency[26], the principle of purpose limitation[27], data minimisation[28], storage limitation[29] and data accuracy[30]. According to the principles of lawfulness, fairness, transparency there must be a legal basis for the processing of personal data. Processing personal data without a legal basis would violate the right to private life. If there is no legal basis, the processing of personal data is not allowed[31]. Also data processing should be done on the basis of fairness and should be guided by the principle of transparency. To guarantee transparency,

[21] Art. 3 Abs. 1 GDPR.
[22] Art. 4 GDPR.
[23] DFKI/Bitkom e. V., Künstliche Intelligenz: Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, 2017, p. 132.
[24] Art 4 and 24 GDPR.
[25] DFKI/Bitkom e. V., Künstliche Intelligenz: Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, 2017, p. 133.
[26] Art 5 §1 a) GDPR.
[27] Art 5 §1 b) GDPR.
[28] Art 5 §1 c) GDPR.
[29] Art 5 §1 e) GDPR.
[30] Art 5 §1 d) GDPR.
[31] DFKI/Bitkom e. V., Künstliche Intelligenz: Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, 2017, p. 134.

the GDPR obliges the responsible person to inform the affected person about the fact of the processing of his data[32], as well as gives him the right of providing information[33]. According to the principle of purpose limitation, personal data should be used only for clear, legitimate and pre-defined purposes. Also according to the principle of data minimization the amount of personal data processed should be in proportion to the pursued purpose. Whereas according to the principle of storage limitation personal data must be stored for as long as necessary to achieve the purpose for which they are collected. Upon reaching the goal these data must be deleted. And finally according to the data accuracy principle the data should be kept up to date and faultless[34].

Generated data can be collected also anonymously. Anonymized data does not fall within the scope of the GDPR. However, even in cases where data collection is done anonymously, the source of the information can be traced, and the privacy of personal data can be violated[35]. These are cases that require in-depth knowledge of experts in the field, are cases that constitute legal violations and have nothing to do with regulatory shortcomings of the legal framework. In technical language they are called pseudonymized data. Pseudonymized data fall within the scope of application of the GDPR[36]. Violation of privacy in such cases constitutes a violation of the right to data protection and the right to privacy in general.

## Conclusions

Automated processing of information is already a necessary good, without which there can be no further scientific and social development. Even public administration in this period of global development of computerized systems cannot do without automated systems for information processing. Automated

[32] Art 13 GDPR.
[33] Art 15 GDPR.
[34] Art 5 GDPR.
[35] Rocher, L., Hendrickx, J. M. and de Montjoye Y. (2019), Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications 10, No. 3069.
[36] DFKI/Bitkom e. V., Künstliche Intelligenz: Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, 2017, p. 133.

data processing apparently improves service to the citizen. Proper data management is important in order not to violate data protection rights.

An important step has been taken with the implementation of the General Data Protection Regulation of 2016. However, it does not touch on all aspects of data processing. Thus, anonymous data do not fall within the scope of the General Data Protection Regulation. The GDPR is guided by general principles of data protection and does not explicitly provide rules relating to the use of algorithms or artificial intelligence in general. Difficulty consists in defining the boundary between de-anonymized or pseudonymized data and anonymized data, on which the application of the directive depends. Defining a clear boundary in this aspect and the continuous improvement of the legal framework, which should follow the steps of technological development, is a necessary condition for the protection of personal data and the non-infringement of the right to privacy.

## References

DFKI/Bitkom e. V. (2017). *Künstliche Intelligenz: Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung.*

CJEU, Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke and Eifert GbR and Hartmut Eifert, Opinion of Advocate General Sharpston, 17 June 2010, para. 71.

Eberl, Aus Politik Und Zeitgeschichte 6–8/2018.

FRA. (2018). *Council of Europe and EDPS (2018), Handbook on European data protection law.* 2018 Edition, Luxembourg, Publications Office.

FRA. (2020). *Getting the future right – Artificial intelligence and fundamental rights.* 2020 Edition, Luxembourg, Publications Office.

Regulation (EU) 2016/679 of the European Parliament and of the Council.

Rocher, L., Hendrickx, J. M., Montjoye Y. (2019). *Estimating the success of re-identifications in incomplete datasets using generative models*, Nature Communications 10, No. 3069.

Russell/Norvig. (2010). *Artificial Intelligence.* A Modern Approach.

Surden, Concurring Opinions. (2012). *https://samirchopra.com/2012/01/31/concurring-opinions-online-symposium-for-a-legal-theory-for-autonomous-artificial-agents/ <04.06.2021>.*

UN, Human Rights Committee, General Comment No. 37. *(2020) on the right of peaceful assembly (article 21), CCPR/C/GC/37, 17 September 2020, para.* 62

Unger/Ungern-Sternberg. (2019). *Demokratie und künstliche Intelligenz, 2019.*

Vermeulen, M. (2014). *SURVEILLE Deliverable D4.7* – The scope of the right to private life in public places, July 2014.