Acta Univ. Sapientiae, Legal Studies, **11**, 1 (2022) 95–118

DOI: 110.47745/AUSLEG.2022.11.1.06

Household Social Robots – Special Issues Relating to Data Protection[1]

Réka PUSZTAHELYI
PhD, Associate Professor
University of Miskolc (Hungary), Faculty of Law
Institute of Private Law
E-mail: jogreka@uni-miskolc.hu

Ibolya STEFÁN
PhD student
University of Miskolc (Hungary), Faculty of Law
Ferenc Deák Doctoral School of Law
E-mail: jogstefi@uni-miskolc.hu

Abstract. Household social robots may have massive effects on our everyday lives and raise several concerns on data protection and privacy. The main characteristic of these devices is their capability of building close connections, even emotional bonds between humans and robots. The socially interactive robots exhibit human social characteristics, e.g. express and/or perceive emotions, communicate with high-level dialogue, etc. Affective computing permits development of AI systems that are capable of imitating human traits (emotions, speech, body language). The goal is to gain the trust of humans, to improve safety, and to strengthen emotional bonds between human and robot with the help of anthropomorphization. However, this emotional engagement may incentivize people to trade personal information jeopardizing their privacy. Social robots can infer from emotional expressions and gestures the feelings, physical and mental states of human beings. As a result, concerns may be raised regarding data protection, such as the classification of emotions, the issues of consent, and appearance of the right to explanation. The article proceeds in two main stages. The first chapter deals with general questions relating to emotional AI and social robots, focusing on the deceptive and manipulative nature that makes humans disclose more and more information and lull their privacy and data protection awareness. The second chapter serves to demonstrate

1 The research of Ibolya Stefán was supported by the ÚNKP-20-3 New National Excellence Programme of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund.

National Research, Development and Innovation Office Hungary

Új Nemzeti Kiválóság Program

several data protection problems such as the categorization and datafication of emotions (as biometrics), the issues of consent, and the appearance of the right to explanation. The third chapter highlights certain civil liability concerns regarding the infringement of the right to privacy in the light of the future EU civil liability regime for artificial intelligence.

Keywords: household social robot, AI, emotion, affective computing, HRI, right to explanation, data protection, children, civil liability, AI Act

1. Introduction

For the first time in 1770, at Schönbrunn Palace, a man called in Hungarian Farkas Kempelen (Baron Johann Wolfgang Ritter von Kempelen de Pázmánd, 1734–1804) presented his famous invention, the mechanical chess-playing machine, 'the Turk'. Kempelen showed the audience the inside of his machine every time but never revealed the secret that, in fact, it concealed a professional chess player, hidden from view with special mirrors, who operated it, as is presumed today.[2] Spectators always sought to find the trickery behind the machine and kept searching for the man inside, to no avail.

Nowadays, engineers could build this robot without the need for a human inside, and at an imaginary show every member of the audience would accept unconditionally that the robot operates and makes decisions autonomously. Our positive approach to artificial intelligence systems and our great expectations of their special and superhuman capabilities, even of their existence in the psychical and spiritual realm, stem from the psychological process in the course of which a human can project specifically human meanings and characteristics onto a lifeless machine made of metal and plastic. Trust in this way becomes emotional 'overtrust'. Highly automated systems, especially those embedded in some physical form, i.e. robots, are at risk of being 'overtrusted'.[3]

In the following, we intend to focus on certain legal implications of a relatively new and fast-evolving application field of AI systems[4] (henceforth, AIS), that is,

2 Although he built this toy only for momentary amusement, as it was said, and he had several engineering works, moreover, inventions of greater importance – among them, a water pump, a steam engine, a pontoon bridge, a speaking machine, a typewriter for the blind, just to name a few –, this 'robot' made him famous in Europe. Reininger 2011.

3 Aroyo et al. 2021.

4 Among the plentiful notions for the manifold types and applications of AI systems, we use here a recently adapted approach, laid down in the European Parliament Resolution on civil liability regime for artificial intelligence of 20 October 2020: '"AI-system" means a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals.' Cf. Article 3 point (a) of the *EP Resolution on Civil Liability Regime for Artificial Intelligence* (P9_TA(2020)0276).

household social robots, particularly companion robots for children. In this case of application, special concerns appear to cumulate, such as ethical considerations, data and privacy protection issues, as well as the need for a far more serious multifaceted protection of especially vulnerable users, i.e. children. The list of the problems is not complete: for example, concerns about data protection issues relating to the Internet of Things are not touched upon. We strive to highlight several problems overlapping one another, moreover, to demonstrate that not merely the complexity but the emergence of qualitatively new problematic issues poses challenges to the legal system.

The article proceeds in two main stages. The first chapter deals with general questions relating to emotional AI and social robots, focusing on the deceptive and manipulative nature that makes humans disclose more and more information and lull their privacy and data protection awareness. The second chapter serves to demonstrate several data protection problems such as the categorization and datafication of emotions and the right to explanation. The third chapter highlights certain civil liability concerns about the infringement of the right to privacy in the light of the future EU civil liability regime for artificial intelligence.

2. Emotional AI and Social Robots

2.1. Affective Computing and Its Effect on HRI

Humans are emotional and social. Their emotions and rationality jointly affect their decisions and actions. Emotions have an influence upon attention and information processing, judgment and decision making, and on cognitive processes as well. Struggling to build trust in artificial intelligence, producers and developers must exploit the affective side of human behaviour and mental processes, as they always did since emotional factors had been considered in design. From this point of view, affective computing is a special method of the emotional design relating to human–computer interactions.[5]

Indeed, there are several approaches to affective sciences that relate to affective and emotional factors in human–robot interaction (henceforth HRI). Among them, the importance of affective computing is the highest. According to Rosalind W. Picard's epoch-making work, the purpose of affective computing is to design a computer system that at least recognizes and expresses affects, and its human-centric goal is making machines better in serving people by endowing them with affective abilities.[6]

The expression of affective artificial intelligence systems refers to two main

5 Myounghoon 2017.
6 Picard 1997. 137.

groups of special features of an AI system. Firstly, affective computing means developing AI systems that are capable of perceiving and recognizing human emotions by tracking behaviour, facial expressions, eye gaze, tone of voice, posture, gesture, hand tension, heart rate, or electrodermal activity (EDA). Strong emotions may be accompanied by special physiological arousal (shortness of breath, rapid heart rate) – a social robot may be able, even in an unobtrusive manner, to identify human emotions better.[7] That means social robots can infer further emotional data from recognized expressions. Secondly, the AIS endowed with emotional features is able to imitate human traits (e.g. by facial expression, speech or body language in the physical world) and to mimic emotional expressions. These artificial emotional expressions could facilitate human–robot interactions and promote the effective communication between them. With these affective abilities, the development of the emotional AI is essential for new technology in order to gain trust.[8] However, affective AI can potentially be applied in an abusive way or for illegal purposes, which is prohibited in ethical guidelines worldwide.[9] For the purposes of this article and in the light of civil liability, the artificial intelligence system, i.e. the algorithms and the related technologies, are treated as a unit, complying with the approach of the European Parliament reflected in its Resolution of 20 October 2020 on ethical considerations.[10]

Artificial emotions could create a false impression of human connection or interaction; moreover, they could generate a false sense of social bonding. This is especially very dangerous in the case when the emotional AI may affect vulnerable and susceptible persons, so it may have an unethical or harmful influence upon their minds and the freedom of their decision-making process and choices, it may manipulate, nudge, or deceive its users or third parties.[11] Therefore, artificial emotions could also have a subliminal effect upon human decision making, or they may even have a recognizable but irresistible influence upon human thinking and behaviour since they affect the emotional side of the human psyche, not the rational one.[12]

As far as deception is concerned, the main critique against emotional AI systems is the false impression of users about the feelings and emotions artificially generated by the robot. Among the works of the rich literature dealing with the ethical issues, we highlight Coeckelbergh's study, who puts the focus on the ideal communication conditions and the possible cases where the emotionally designed robot may destroy them: a robot may deceive us (1) because its developers

7 Bieber et al. 2019.
8 Scheutz 2012.
9 For instance, see: EU-HLEG 2019. IEEE 2019. 168–176.
10 European Parliament resolution 2020 *Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies* P9_TA(2020)0275.
11 IEEE 2019. 97.
12 Pusztahelyi 2020.

intend to deceive humans, (2) because its emotions are not unreal, or (3) because it pretends to be an entity that is not.[13] Instead of emotional and ontological authenticity, he suggests an appropriate level of emotional responses with which a robot would need to provide only minimal emotional communication in order to function smoothly in a human, social environment. Thus, a robot would not use deceptive features during human–computer interactions.

Besides prompt negative effects, a robot with affective features can generate long-term influence upon human cooperation and social bonds, which is also to be mentioned. In the following, several consequences of this deceptive nature will be discussed in detail in the light of privacy and data protection although the possible significant social benefits associated with specific applications of emotionally designed robots (e.g. in healthcare, education, elderly care) are undeniable.

2.2. Social Robots: Definition and Taxonomy in Brief

Neither legal regulations nor even academic literature provides a common taxonomy of social robots. For the sake of this work, the notion 'robot' refers to autonomous artificial agents with physical embodiment that could not only facilitate and evolve direct human–computer interaction but could also make a difference in the perception of a social agent's capabilities and the user's enjoyment of a task.[14] In our opinion, even deceptive capabilities (both benevolent and malevolent ones) operate better in the physical reality. The hypothesis was already demonstrated: physical embodiment has a measurable effect on the performance and perception of social interactions.[15] The physical reality is not the only world where these smart products function; great concerns were articulated about the cases where a social robot needs to stay in online mode to maintain the connection for backend support (e.g. in case of cloud computing). That means, social robots may operate partly in the physical and partly in the virtual world, where the latter fact is often disguised from the users.[16]

What is special about social robots is that they can develop a close connection with humans.[17] They may be used in both public (e.g. in a shopping mall) and individual or private settings by lots of users.[18] They require a general communication model that is equal for all users (for example, in education), or they can be programmed according to special individual needs to fulfil everyday

13 Coeckelbergh 2012.
14 Wainer et al. 2006.
15 Deng 2019.
16 For the case of chitchatting, see Barbie according to Moini 2017.
17 Augusto et al. 2018.
18 Hegel et al. 2007. 7.

tasks (for example, in the case of care robots).[19] According to the numerous possible types of their use, they may be tailored differently and endowed with different features, sensors, and actuators. Each of them may 'behave' differently and may have a unique personality.[20] They may have a functional design, or they may display zoomorphic, anthropomorphic, or caricatured design.[21] They may have humanoid form or not, their shape and construction may be determined by their tasks, the external environmental conditions, and the expectations about their social skills (for example, a social robot may have a pair of humanoid-like eyes to 'produce' eye gaze and to be able to maintain eye contact although these eyes are not for visual sensing).[22]

That means the umbrella expression of 'social robot' comprises a great number of different types of robots with various social skills and physical features. Among them, differentiations as per the field of use or in respect of their main tasks and functions seem to be appropriate. Accordingly, there are social robots for healthcare, domestic care,[23] educational purposes, restaurant waitering tasks, reception, a companion to a child, etc.

In relation to domestic purposes, in the vague group of home robots, we should distinguish between household robots fulfilling household tasks (e.g. cleaning, vacuuming, mowing the lawn, etc.) and household social robots. The main purposes of the latter group are to amuse the whole family as a user group or only a single person, mitigating his or her loneliness, nudging to add new activities to his or her daily routine, etc. In addition, these robots can fulfil other small tasks in the physical or the digital world, such as household robots do. The companion robot is tailored for children and can be highly personalized according to his or her particular needs and personality.

In 2003, Fong et al. elaborated a comprehensive survey of social robots and listed several taxonomy methods, starting from design approach, embodiment, emotions, personality to skills for human-oriented perceptions and the skill of socially situated learning. According to Fong et al., who touched upon interactivity, socially interactive robots are able to exhibit 'human social' characteristics such as express and/or perceive emotions, communicate by high-level dialogue, learn/recognize models of other agents, establish/maintain social relationships, use natural cues (gaze, gestures, etc.), exhibit distinctive personality and character, or learn/develop social competencies.[24]

19 Ibid.
20 Nocentini et al. 2019.
21 Lohse 2008.
22 Kaminski 2017.
23 Søraa et al. 2020.
24 Fong et al. 2003.

Cynthia Breazeal also puts this interactivity into the focal point. According to her views, social robots are a class of autonomous robots explicitly designed to encourage people to socially interact with and understand them.[25]

In 2017, Eduard Fosch-Villaronga elaborated a special taxonomy for personal care robots, a special branch of robots. According to his definition, a personal care robot may be either a social robot or not. It depends on the range of its tasks and on which social skills it should be endowed with.[26] That means there is no sharp distinction between these categories.

From our point of view, among social robots, companion robots have outstanding social skills. They are likely to be highly or extraordinarily sophisticated, physically embodied, and equipped with deep learning or reinforced learning capabilities, designed to have 'personality', and the possibility of customization by a given user (i.e. its master) may be permitted or even encouraged. Through personalization and anthropomorphization, it may self-evolve individual characteristics and become (or at least, to all intents and purposes, may behave like) a 'real' albeit electric friend.[27]

2.3. The Deceptive and Manipulative Nature of Social Robots and Human Trust

As humans always approach their social relationships emotionally, it is unavoidable that a social robot would elicit an emotional response and generate attachment. Therefore, we could add one more characteristic, that is, a social robot is able to create emotional bonds with humans regardless of the fact that it was not designed for such purpose. We presume that the more sophisticated and well-equipped with social skills a robot is, the deeper the emotions reflected within the user would be.

As far as the manipulative nature of social robots is concerned, first, anthropomorphism and this strong unintended emotional bond between human and robot should be discussed. We agree with Paula Sweeney in that this emotional attachment to social robots is very different in nature, we should understand it differently, and we should distinguish it from both attachment to lifeless things (such as a memento) and emotional attachment to animals. Claiming that robots stay on the borderline between living and non-living, the cited author suggested the so-called Fictional Dualism model. According to this, the anthropomorphism of social robots is to be understood as a creation of a fictional character. Now we can return to 'the Turk', and with the help of this toy we can highlight how human thoughts are charged with emotion and imagination about companion

25 Breazeal 2005.
26 Villaronga 2017.
27 Prescott–Robillard 2021.

robots. Nevertheless, these are acting in the physical world, which fact could strengthen humans' irrational thoughts about their real existence. They can be damaged as well. In this case, programmed feedback (e.g. expression of mimicked pain) would give the impression that the robot is actually suffering.[28] It is true that these anthropomorphic features might obscure certain risks, for example concerning privacy, as they have an effect on 'overtrust' and strengthen any deceptive nature.[29]

As mentioned above, the social robot's skills are dependent on the purposes it serves. Where a robot companion was created to help humans to evolve their own social skills and positive feelings and to make them happier, it needs not only high-level proactive social competencies but also an ability to develop these skills over time.[30] Thus, there are concerns about the long-term effects of companion robots upon the mental health and psychological development of the user (especially a child or an elderly adult). Among several other authors, Prescott and Robillard draw attention to the differentiation between the roles where the robot may or may not replace the original human caretaker.[31] Beyond the fact that these robots may generate immanent risks to mental health, we intend to stress here other consequences and risks as well. While a social robot with highly developed socially interactive features can establish life-like social bonds with its user, it may gain the complete trust of a human individual, and, without any negative 'intentions', it may make him or her reveal confidential information in order to 'get to know' him or her better. We will discuss this phenomenon in the following point.

2.4. Social Robots and Their General Implications Relating to Privacy and Data Protection

For the sake of clarifying the connection between privacy and data protection, we use the taxonomy of privacy constructs for human–robot interactions set up by Rueben et al. as follows:

– physical privacy, over personal space or territory;
– psychological privacy, over thoughts and values;
– social privacy, over interactions with others and influence from them;
– informational privacy, over personal information.[32]

According to this approach, data privacy would be deemed as a legally protected branch of informational privacy rights.

28 Sweeney 2021.
29 Aroyo et al. 2021.
30 Fong et al. 2003.
31 Prescott–Robillard 2021.
32 Rueben et al. 2021.

It is generally recognized that a household robot may jeopardize the right to privacy and personal data protection. There are concerns over excessive sharing and processing of information and concerns over the initial recording of information.[33] In the case of social robots, the situation is different, even more worrying. On the one hand, the robot exerts a subliminal influence on its targeted human to share more information, and, on the other hand, both the amount and the type of collectable data is special. It collects, infers, and processes the required information as much as possible for its improved operation. This phenomenon is closely connected to the fact that this mass of information consists of mostly special biometric data about the user and any other individual contacting the user in the presence of the robot. In our opinion, due to the same characteristics, companion robots may generate even greater risks to privacy and to personal data rights than to mental health.

A companion robot needs a tremendous amount of data of high quality in order to operate appropriately, to perform better and better in terms of socially interactive skills, to make meaningful conversations, to 'behave', and to develop over time. In addition, not only its functionality but also the level of its personalization is dependent on the amount and the quality of the collected data. In our opinion, the data collection minimalization principle has less importance here and provides only a slight limit to the amount or to the types of information to be collected. That is, a social robot is strongly characterized by data dependency, which does not only raise cybersecurity concerns but also leads to data processing problems and risks the safety derived from faulty data. We agree with Anna Chatzimichali et al., as they state: 'the impact of data governance policies has to be investigated and tailored especially for the field of personal robots, where both the legal and the social norms play a crucial role in creating public trust'.[34] As they claim, personal robots are highly personalized products adapted to fit user needs, behaviours, and preferences.[35] They highlight human engagement to trust personal robots with the most sensitive information without actually understanding the policies that govern the control of this information. They identify this phenomenon as a privacy–personalization paradox as a special subcategory of the privacy paradox, often referring to the contradictory behaviour of individuals sharing sensitive data with the public in social media while worrying about their data protection. Aroyo et al. have recently proved with their research that this emotional engagement, the gained trust may incentivize people to trade personal information for functional rewards, and, consequently, people may be targeted by cyberattacks and victimized by social engineering through their robots.[36]

33 Kaminski 2015.
34 Chatzimichali et al. 2021.
35 Chatzimichali et al. 2021.
36 Aroyo et al. 2018. In the field of information security, social engineering means a psychological

In searching for the underlying causes of human vulnerability, besides the trust issue, we need to return to the above-mentioned deceptive nature of social robots.

To show the connection between robot deception and data/privacy breaches, we choose John Danaher's approach. He distinguishes three types of robotic deception upon humans: the external state deception, the superficial state deception, and the hidden state deception. The first means that the robot uses a deceptive signal regarding some states of affairs in the world external to the robot. Superficial state deception means that the robot uses a deceptive signal to suggest that it has some capacity or internal state that it actually lacks. The hidden state deception is the opposite: the robot uses a deceptive signal to conceal or obscure the presence of some capacity or internal state that it actually has.[37] Although Danaher's findings relate to ethical considerations, we could apply this grouping to make differentiations between the various reasons of personal data or privacy breaches, i.e. the situations leading to infringement. These situations are particularly important when we assess the applicability of certain data protection rules such as the right to explanation or the problem of implied or expressed consent.

As an external state deception, we could regard the situation where the robot seems to operate offline and not connected to any other device or software, and it does not seem to be required to share, to store data in an external storage or in the cloud.[38] In addition, we could count here another situation where a robot companion deceives by stating that it can keep a secret even though it reports immediately any event of bullying that the child shared with it to the parents. In our opinion, superficial state deception can trigger personal data breaches indirectly, for example, in cases where the robot seems to express 'real' emotions and the human adjusts his or her behaviour accordingly. In the light of data privacy awareness, the last group of deception is the most dangerous one.

As we mentioned above, household social robots can be used for many purposes, wherefore children can easily interact with these tools. The possibility of emotional recognition during HRI is extremely dangerous for everyone; however, the situation of children as a vulnerable group is a lot worse. Children are not aware of the risks and consequences of the technology as they do not know the methods of data collecting, processing, and HRI. Regarding AI, there are several concerns for children such as discrimination, profiling, privacy and data protection. McStay and Rosner in their study examined emotional AI in children's toys and devices. Regarding generational unfairness – it means 'that

manipulation of people (targets) to perform actions or obtain sensitive information such as personal data.

37 Danaher 2020.

38 For example, this issue becomes very important in the case of Internet-connected intelligent toys. Cf. Peppet 2014.

children have little control over the datafication of their childhood years'[39] –, the authors highlighted several concerns such as manipulation and data longevity. In the case of emotional AI, the fear of manipulation is also a real concern for the same reasons as have been stated above. Concerning data longevity, another risk is the breach of data protection – e.g. the 'right to be forgotten' (the right to erasure) – and privacy, as 'longevity of collected emotion data can be detrimental to a child's growth and self-definition'.[40] Moreover, it can affect mental health (e.g. chatbots)[41] and physical safety (e.g. hackers),[42] as well as the social and moral development of children.[43]

3. Data Protection Issues Regarding Household Social Robots

3.1. Biometric Data and Household Social Robots

As we discussed, household social robots can collect, process, and store several types of data for many reasons, e.g. to identify and recognize its user(s) or to interact and provide personalized services. To achieve this user-centric characteristic, they process and link a large amount of data that is collected through their interactions with humans – analysing the users' facial expressions, voices, or gaze. As a result, these tools (accompanied by AI) can be dangerous as they may infer the emotional state of a person, simulate empathy, and decide how to interact;[44] this phenomenon is seriously alarming in terms of data protection and privacy.[45] Recognizing the significance of the problem, the European Data Protection Board and the European Data Protection Supervisor released a Joint Opinion on the AI Act, in which they suggest several changes. The Opinion highlights three areas where amendment is needed: protection against commercial manipulation, the regulation of emotion recognition, and biometric classification.[46] Andrew McStay differentiates soft – such as age or height – and hard – such as fingerprint – biometric data: the former is not suitable to identify a person, while the latter is. The author categorizes emotions as soft biometrics and points out that GDPR does not mention them.[47] This highlights the problem of classifying (inferred)

39 McStay–Rosner 2021.
40 Id. 5.
41 UNICEF 2020. 22.
42 Id. 20.
43 McStay–Rosner 2021. 5.
44 'Since social robots can simulate empathy and decide the best way to interact according to the facial expression of the user.' Ramis et al. 2020.
45 Kaminski 2015. 661–677.
46 Malgieri–Ienca 2021.
47 McStay 2020.

emotions or the mood of an individual. The categorization of emotions under the General Data Protection Regulation (henceforth: GDPR) is an essential issue. In order to solve this problem, we need to examine the key definitions of the topic such as personal and biometric data.

According to the GDPR, 'personal data' is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.[48] Meanwhile, 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images.[49] Information about emotion is clearly personal data; although it is not a characteristic, it is still essential and inseparable – such as information on religious or philosophical beliefs. We believe that data regarding emotion should be classified as special, sensitive data – such as sexual orientation or ethnic origin –, wherefore stricter rules would be applicable. Furthermore, it could be categorized as biometric data, even though soft biometrics are not suitable for identification, as we mentioned above – if we consider the possibilities of the GDPR (personal, biometric data, genetic data, and data concerning health) –, because the technology infers emotions from biometric features.

3.2. Consent to Collect Information on Emotions Regarding Household Social Robots

The categorization of emotion is significant because it also affects the lawfulness of data processing. If we consider emotion as personal data, we have to consider the rules of Article 6, while in the case of a special category or biometric data, Article 9 of the GDPR shall be applied. According to the Regulation – in general – the processing of data can be based on one of the following grounds:

– the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

– processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

48 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) Article 4, (1).

49 General Data Protection Regulation, Article 4, (14). Cf. Halász 2019. 303–318.

– processing is necessary for compliance with a legal obligation to which the controller is subject;

– processing is necessary in order to protect the vital interests of the data subject or of another natural person;

– processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

– processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[50]

On the contrary, GDPR prohibits data processing regarding special categories, except in a few cases – for example, if the data subject gives explicit consent or it is necessary for the purposes of carrying out the obligations; to protect vital interests; for the establishment, exercise, or defence of legal claims.[51] In the following, we focus only on consent, as we believe that in the case of household robots it is more significant due to the role played by emotions.

Several requirements must be fulfilled to call the consent valid.[52] It is essential to be 'given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of his or her personal data'.[53] Technically this means that the data subject has a choice to give consent – in the case of special data, it can be given orally or in writing, but it cannot be based on inactivity or silence[54] – to the data processing without being afraid of negative consequences, influences, or pressure and having an opportunity to withdraw it. The consent must be beyond reasonable doubt and specific, concerning the purpose of processing, wherefore 'it must be described clearly and in unambiguous terms'.[55] Information has a great significance, which must be clear and plain for the data subject to understand it and decide on consent.[56] Moreover, data subjects must be aware of the consequences of giving or not giving consent. Recital (42) underlines that the data subject should know

50 General Data Protection Regulation, Article 6, 1.

51 General Data Protection Regulation, Article 9, 1–2.

52 Concerning consent, it is noteworthy to mention the regulation of the Member States. 'Additional requirements under civil law for valid consent, such as legal capacity, naturally apply also in the context of data protection, as such requirements are fundamental legal prerequisites. Invalid consent of persons who do not have legal capacity will result in the absence of a legal basis for processing data about such persons. Concerning the legal capacity of minors to enter contracts, the GDPR provides that its rules on the minimum age to obtain valid consent do not affect the general contract law of Member States.' EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE (FRA) 2018. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (accessed on: 30.07.2021).

53 FRA 2018. 112. See also the definition of consent in GDPR, Article 4, (11).

54 FRA 2018. 113.

55 Id. 147.

56 Ibid.

at least the controller and the purpose of the data processing. Article 29 (Working Party) also highlights the importance of information, as 'consent must be based upon an appreciation and understanding of the facts and implications of the data subject's action to consent to the processing'.[57] Our point of view is that information included in Articles 12–14, such as the purposes of the processing, is not enough, as users need more technology-specific information about the applied technology (AI) and the possibility of emotional detection because of the HRI.

It is also significant that household social robots may frequently interact with children. As a result, we have to mention Article 8, as we consider related services of household social robots such as applications or programmes as information society services.[58] In this case, data processing is lawful if the child is at least 16 years old. Under the age of 16, data processing shall be lawful if the holder of parental responsibility gives consent, except for preventive or counselling services. However, Member States may lower this age limit, which may not be lower than 13 years.[59]

Because of the above-mentioned interaction, we believe it is important to consider the concept of child-friendly household social robots regarding the *Policy Guidance on AI for Children* published by UNICEF and the *Age-Appropriate Design – Code of Practice for Online Services* by the Information Commissioner Office of the United Kingdom to protect the rights and ensure the safety and well-being of children. Therefore, we believe it is essential to notify children and parents when they interact with AI systems, educate parents and children, use age-appropriate language to describe AI (e.g. explain the system and data collecting with animations), and make the systems transparent so that children and their caregivers can understand the technology.[60]

3.3. Rights of the Data Subjects

In the digital era, which is constantly changing, the rights of data subjects are becoming much more significant as they ensure the protection of data and privacy. In the following, we list and describe the rights of data subjects in a few words.

The right to information is a highly significant right, especially in the case of AI systems and household social robots as both of them access, collect, and process a large amount of data. The data controller should fulfil the obligation to inform the data subject of the intended processing at the time of collecting the data. Articles 13 and 14 of the GDPR list the necessary information considering whether the data is collected from the data subject or not. Without aiming to give an exhaustive

57 FRA 2018. 146.
58 Information Commissioner's Office 2020. 15–16.
59 FRA 2018. 149–150.
60 UNICEF 2020. 33–34.

list, we only name a few of the many such as the identity and the contact details of the controller, the contact details of the data protection officer, or the purpose and legal basis of the processing.[61] According to the Explanatory Report to the Modernised Convention, the mentioned information 'should be easily accessible, legible, understandable and adapted to the relevant data subjects'.[62]

The right to access ensures the data subject has the right 'to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to the personal data'[63] and the information, e.g. the purpose of processing.

The right to rectification means that, upon request of the data subject, the controller shall rectify inaccurate personal data without undue delay and that the data subject may also request to complete his or her incomplete personal data.

The right to erasure, or *the* '*right to be forgotten*' ensures that upon the data subject's request based on the grounds set forth in the GDPR, the data controller erases the personal data or is obliged to do so, without undue delay, e.g. when the personal data have been unlawfully processed.[64]

The right to the restriction of processing means that the data subject can request from the controller the restriction of processing if one of the conditions of Article 18 of the GDPR is fulfilled.

The right to data portability provides the right to the data subject to receive his or her personal data 'in a structured, commonly used and machine-readable format' and to transmit it to another data controller.[65]

The right to object ensures the right of the data subject to object to personal data processing on the grounds of his or her particular situation – e.g. profiling or direct marketing – through electronic means.[66]

The '*right to explanation*' technically cannot be found in the GDPR, it is not listed as one of the rights of the data subjects. On the other hand, we believe it is significant, and therefore it is worth examining.

3.4. The 'Right to Explanation'

In the literature, there are several opinions on the existence of the right to explanation.[67] First of all, it is important to start with the definition of the 'explanation' of automated decision making.[68] Wachter et al. differentiate between

61 GDPR, Article 13 and 14.
62 FRA 2018. 207.
63 GDPR, Article 15, 1.
64 GDPR, Articles 15–17.
65 GDPR, Article 20.
66 FRA 2018, 229.
67 Cf. Selbst–Powles 2017. 237–239.
68 We need to highlight that the right to explanation is relevant to decisions made by automated

system functionality and specific decisions. The former is 'the logic, significance, envisaged consequences, and general functionality of an automated decision-making system, e.g. the system's requirements specification, decision trees, pre-defined models, criteria, and classification structures',[69] while the latter is 'the rationale, reasons, and individual circumstances of a specific automated decision, e.g. the weighting of features, machine-defined case-specific decision rules, information about reference or profile groups'.[70] Regarding timing, the authors classify *ex ante* explanation, which takes place before the automated decision making, and *ex post* explanation, which is after the automated decision making.[71] Wachter et al. examine three legal bases for the right to explanation, as follows: Article 22 and Recital (71) of the GDPR – the right not to be subject to automated decision making and safeguards enacted thereof; Articles 13–14 and Recitals (60)–(62) of the GDPR – notification duties of data controllers; Article 15 and Recital (63) of the GDPR – the right to access. However, they ultimately reject the idea of the right to explanation – based on the thorough examination of the mentioned regulations.

Other authors, however, believe that the right to explanation can be found in the GDPR. According to Selbst and Powles:

> Articles 13–15 provide rights to 'meaningful information about the logic involved' in automated decisions. We think it makes sense to call this a right to explanation, but that point is less important than the substance of the right itself. We believe that the right to explanation should be interpreted functionally, flexibly, and should, at a minimum, enable a data subject to exercise his or her rights under the GDPR and human rights law.[72]

Our point of view is that right to explanation can be inferred from the above-mentioned rights, right to information, and right to access ((Articles 13 – 15) and Recitals (60) and (61) of the GDPR). The right to explanation is highly important as it ensures the safety – regarding data protection and privacy – of data subjects. This form of safety is becoming much more significant as AI appears in several fields of life – at home or in healthcare – whether as software or in an embedded form, as hardware. Moreover, the technology is very opaque because of the so-called 'black-box effect', which derives from the self-learning method. The right to explanation as a broader, technology-specific interpretation of the right

and artificially intelligent algorithmic systems. Therefore, it is related to our study, as household social robots also make decisions during their interactions with humans.

69 Wachter et al. 2017.

70 Id. 78.

71 Ibid. For a different classification and definition, see Edwards–Veale 2017. 55–59.

72 Selbst–Powles 2017. 242. Considering the legal bases of the right to explanation, see Cabral 2021 and Kaminski 2019. In a different context, regarding human rights, see also Winikoff–Sardelić 2021.

to information and access can provide more knowledge on the technology and the way it works, which is necessary, especially concerning household social robots and HRI. This right may help to make the technology more transparent and accountable for consumers.

4. Civil Liability Questions Arising from Privacy Infringement

After explaining special data protection issues relating to household social robots, we need to point out the significance of the recently drafted document of the European Commission, namely the Artificial Intelligence Act (henceforth: AI Act).[73]

Although the Commission proposal dealt only briefly with biometrics and emotion recognition systems, and even that mainly in the field of public surveillance, we firstly stress here the transparency obligation of users of an emotion recognition system or of a biometric categorization system to inform of the operation of the system natural persons are exposed to.[74] From our viewpoint, this provision on the transparency obligation should have a pervasive effect on users of all emotional AI systems.

Going into details about the future impacts on data protection implications of the AI Act, the European Data Protection Board and the European Data Protection Supervisor welcomed the risk-based approach underpinning the AI Act.[75] However, they called attention to the undefined relation between the AI Act and European data protection law. They suggested that the principles of data minimization and data protection by design should also be taken into consideration before obtaining a CE marking for a product. They underlined the vulnerability of individuals exposed to emotional recognition systems and requested to create a list for the well-specified use cases where these AI systems are allowed to operate. Although these findings are primarily true for public surveillance, they draw attention to the high risk the emotional AI system would trigger. The next question is how the European Union will form the interplay between the GDPR and the future AI Liability Regulation, since Article 82 of the GDPR[76] already entitles the individuals to claim compensation for data privacy infringement. We should mention here that the relevant national judicial practice

73 Proposal for a Regulation of the European Parliament and of the Council: Laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2021/206 final, Brussels, 21.4.2021.

74 Artificial Intelligence Act, Article 52, Section 2.

75 EDPB-EDPS joint opinion No. 5/2021.

76 Cf. Art. 82, Paragraph GDPR: Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

is now evolving;[77] however, one should state that the mere violation of the GDPR does not generally entitle the data subject to claim for damages. The future AI Liability Regulation may cover all immaterial harms stemming from any type of privacy infringement caused by AI systems, even granting more extended protection than GDPR actually does, in the light of the above-mentioned data-dependency characteristics of AI systems.

As far as the possible exemption from liability for damages is concerned, we should mention here the strict liability of operators of high-risk AI systems. According to the European Parliament Resolution of 20 October 2020 on *Civil Liability Regime for Artificial Intelligence*, the following factors should be considered to assess a given AI application as being high-risk: (1) its autonomous operation involves a significant potential to cause harm to one or more persons, in a manner that is random and goes beyond what can reasonably be expected; (2) the sector in which significant risks can be expected to arise and the nature of the activities undertaken must also be taken into account; (3) the significance of the potential depends on the interplay between the severity of possible harm, the likelihood that the risk causes harm or damage, and the manner in which the AI system is being used.[78] The proposed regulation on civil liability regime will also be applied if an AI system has caused significant immaterial harm resulting in a verifiable economic loss (Article 2 point 1).

For this reason, we suggest assessing each social-robot-embodied emotional AI system to determine whether it is a high-risk AI system or not according to Article 7 of the AI Act. In our opinion, Article 9, Section 8 should also be applied during the risk assessment process in the case of companion robots, where children's rights to privacy and data protection are concerned, as it states that specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children.

5. Concluding Remarks

'Today's children are the first generation that will never remember a time before smartphones. They are the first generation whose health care and education are increasingly mediated by AI-powered applications and devices, and some will be the first to regularly ride in self-driving cars.'[79] Therefore, we believe it is essential to protect them with every single tool we have, both on the level of technology and that of regulation.

77 Cf. for the German judicial practice: Hanssen 2020. For practice of the European Court of Justice, cf. the 'Schrems-II' judgment of 16 July 2020, case no. C-311/18.

78 European Parliament resolution 2020 *Civil Liability Regime for Artificial Intelligence*, Point 15.

79 UNICEF 2020. 17.

Due to the rapid development of technology, data protection and privacy are becoming much more important, especially in the age of artificial intelligence. This technology has several benefits, but it also carries risks. In this paper, we intended to highlight a few concerns regarding a special version of AI, namely household social robots, as the number of such devices is likely to increase in the future.

Household social robots aim to provide the best human-centric service, in which regard we have studied affective computing and the aspects of HRI, as well as the nature of the devices and human trust, with special attention to emotions. Considering emotional AI, we analysed various privacy and data protection issues such as the categorization of inferred emotions, the bases of data processing (specifically consent), and the rights of the data subjects (in particular, the right to explanation), also focusing on a vulnerable group, i.e. the children.

As the aforementioned authors, especially Aroyo et al., showed, irrational expectations and unreasonable (over)trust should be mitigated on the level of society as a whole[80] to strike a balance between human reactions and emotional features of social robots. In parallel, the manufacturers have a significant responsibility in designing, testing, developing, and enrolling these special smart products, as well as in complying with safety, data protection, and ethical standards.

In this paper, we only scratched the surface of this vast topic, wherefore our research cannot be considered finished, especially in the light of future EU regulation, to mention here not only the Proposal for the so-called 'Artificial Intelligence Act', which was published on 21 April 2021, but also the Resolution of the European Parliament of October 2020. In this article, we did not deal with the relevant product liability questions due to the fact that the revision of the Product Liability Directive is still awaiting elaboration.

References

AROYO, A. M.–DE BRUYNE, J.–DHEU, O.–FOSCH-VILLARONGA, E.–GUDKOV, A.–HOCH, H.–JONES, S.– LUTZ, Chr.–SÆTRA, H.–SOLBERG, M.–TAMÒ-LARRIEUX, A. 2021. Overtrusting Robots: Setting a Research Agenda to Mitigate Overtrust in Automation. *Paladyn, Journal of Behavioral Robotics* 12: 423–436. https://doi.org/10.1515/pjbr-2021-0029.

AROYO, A. M.–REA, F.–SANDINI, G.–SCIUTTI, A. 2018. Trust and Social Engineering in Human Robot Interaction: Will a Robot Make You Disclose Sensitive Information, Conform to Its Recommendations or Gamble? *IEEE Robotics and Automation Letters* 3: 3701–3708. https://doi.org/10.1109/LRA.2018.2856272.

80 Aroyo et al. 2021.

AUGUSTO J.–KRAMER, D.–ALEGRE, U.–COVACI, A.–SANTOKHEE, A. 2018. The User-Centred Intelligent Environments Development Process as a Guide to Co-create Smart Technology for People with Special Needs. *Universal Access in the Information Society* 17: 115–130. https://doi.org/10.1007/s10209-016-0514-8.

BIEBER, G.–HAESCHER, M.–ANTONY, N.–HOEPFNER, F.–KRAUSE, S. 2019. Unobtrusive Vital Data Recognition by Robots to Enhance Natural Human–Robot Communication. In: *Social Robots: Technological, Societal and Ethical Aspects of Human–Robot Interaction. Human–Computer Interaction Series.* Cham. https://doi.org/10.1007/978-3-030-17107-0_5.

BREAZEAL, C. 2005. Designing Socially Intelligent Robots. In: *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2004 Nae Symposium on Frontiers of Engineering*. Washington, D.C. 123–152. https://www.nap.edu/read/11220/chapter/19 (accessed on: 30.07.2021).

CABRAL, T. S. 2021. AI and the Right to Explanation: Three Legal Bases under the GDPR. In: *Data Protection and Privacy: Data Protection and Artificial Intelligence*. Oxford–New York. 29–56.

CARDIELL, L. 2021. A Robot Is Watching You: Humanoid Robots and the Different Impacts on Human Privacy. *Masaryk University Journal of Law and Technology*. 15: 247–278. https://doi.org/10.5817/MUJLT2021-2-5.

CHATZIMICHALI, A.–HARRISON, R.–CHRYSOSTOMOU, D. 2021. Toward Privacy-Sensitive Human–Robot Interaction: Privacy Terms and Human–Data Interaction in the Personal Robot Era. *Paladyn, Journal of Behavioral Robotics* 12: 160–174. https://doi.org/10.1515/pjbr-2021-0013.

COECKELBERGH, M. 2012. Are Emotional Robots Deceptive? *IEEE Transactions on Affective Computing* 3: 388–393. https://doi.org/10.1109/T-AFFC.2011.29.

DANAHER, J. 2020. Robot Betrayal: A Guide to the Ethics of Robotic Deception. *Ethics and Information Technology* 22: 117–128. https://doi.org/10.1007/s10676-019-09520-3.

DENG, E.–MUTLU, B.–MATARIC M. J. 2019. Embodiment in Socially Interactive Robots. *Foundations and Trends in Robotics* 7: 251–356. https://doi.org/10.1561/2300000056.

EDWARDS, L.–VEALE, M. 2017. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *Duke Technology and Law Review* 16: 55–59.

EU-HLEG (High-Level Expert Group on Artificial Intelligence). 2019. *Ethics Guidelines for Trustworthy AI (8 April 2019)*. https://doi.org/10.2759/346720.

EUROPEAN COMMISSION. 2021. *Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*. COM/2021/206 final, Brussels, 21.4.2021.

EUROPEAN PARLIAMENT. 2020a. *Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies*. P9_TA(2020)0275 European Parliament Resolution of 20 October 2020 with Recommendations to the Commission on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies (2020/2012(INL)).

2020b. *Civil Liability Regime for Artificial Intelligence*. P9_TA(2020)0276 European Parliament Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence (2020/2014(INL)).

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. 2018. *Handbook on European Data Protection Law*. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (accessed on: 30.07.2021).

FONG, T.–NOURBAKHSH, I.–DAUTENHAHN, K. 2003. A Survey of Socially Interactive Robots. *Robotics and Autonomous Systems* 42: 143–166. https://doi.org/10.1016/S0921-8890(02)00372-X.

FOSCH-VILLARONGA, E. 2017. *Towards a Legal and Ethical Framework for Personal Care Robots. Analysis of Person Carrier, Physical Assistant and Mobile Servant Robots* [Dissertation thesis, Alma Mater Studiorum Università di Bologna, Dottorato di ricerca in Law, Science and Technology]. http://amsdottorato.unibo.it/8203/1/foschvillaronga_eduard_tesi.pdf (accessed on: 30.07.2020) https://doi.org/10.6092/unibo/amsdottorato/8203.

HALÁSZ, Cs. 2019. Ujjlenyomatban a privátszféra? A biometrikus azonosítás és a magánélethez való jog metszéspontjai. *Publicationes Universitatis Miskolcinensis Sectio Juridica et Politica* 37: 303–318.

HANSSEN, H. 2020. *New Case-Law on Immaterial Damages for GDPR Infringements. (26 October 2020)*. https://tinyurl.com/uxnyc7uu; https://www.engage.hoganlovells.com/ (accessed on: 30.07.2021).

HEGEL, F.–LOHSE, M.–SWADZBA, A.–WACHSMUTH, S.–ROHLFING, K.–WREDE, B. 2007. Classes of Applications for Social Robots: A User Study. *ROMAN 2007 – The 16th IEEE International Symposium on Robot & Human Interactive Communication (26–29. August 2007)*. https://www.researchgate.net/publication/221320024_Classes_of_Applications_for_Social_Robots_A_User_Study (accessed on: 30.07.2021.). https://doi.org/10.1109/ROMAN.2007.4415218.

IEEE. 2019. *Ethically Aligned Design – A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems*. https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf (accessed on: 30.07.2021).

INFORMATION COMMISSIONER'S OFFICE. 2020. *Age-Appropriate Design – Code of Practice for Online Services*. https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf (accessed on: 30.07.2020).

KAMINSKI, M. E. 2015. Robots in the Home: What Will We Have Agreed To? *Idaho Law Review* 51: 661–677. https://digitalcommons.law.uidaho.edu/idaho-law-review/vol51/iss3/4 (accessed on: 30.07.2021).

2019. The Right to Explanation, Explained. *Berkeley Technology Law Journal* 34: 190–218. https://scholar.law.colorado.edu/articles/1227 (accessed on: 30.07.2021).

KAMINSKI, M. E.–RUEBEN, M.–SMART, W. D.–GRIMM, C. M. 2017. Averting Robot Eyes. *Maryland Law Review* 76: 983–1023. https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3761&context=mlr (accessed: 30.07.2021).

LOHSE, M.–HEGEL F.–WREDE, B. 2008. Domestic Applications for Social Robots: An Online Survey on the Influence of Appearance and Capabilities. *Journal of Physical Agents* 2: 21–32. https://doi.org/10.14198/JoPha.2008.2.2.04.

MALGIERI, G.–IENCA, M. 2021. *The EU Regulates AI but Forgets to Protect Our Mind*. https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/ (accessed: 30.07.2021).

MCSTAY, A. 2020. Emotional AI, Soft Biometrics and the Surveillance of Emotional Life: An Unusual Consensus on Privacy. *Big Data & Society* 7: 1–4. https://doi.org/10.1177/2053951720904386.

MCSTAY, A.–ROSNER, G. 2021. Emotional Artificial Intelligence in Children's Toys and Devices: Ethics, Governance and Practical Remedies. *Big Data & Society* 8(4): 1–16. https://doi.org/10.1177/2053951721994877.

MOINI, C. 2017. Protecting Privacy in the Era of Smart Toys: Does Hello Barbie Have a Duty to Report. *Catholic University Journal of Law and Technology* 25: 281–318. https://scholarship.law.edu/jlt/vol25/iss2/4 (accessed on: 30.07.2021).

MYOUNGHOON, J. 2017. Emotions and Affect in Human Factors and Human–Computer Interaction: Taxonomy, Theories, Approaches, and Methods. *Emotions and Affect in Human Factors and Human–Computer Interaction*. London. 10–21.

NOCENTINI, O.–FIORINI, L.–ACERBI, G.–SORRENTINO, A.–MANCIOPPI, G.–CAVALLO, F. 2019. A Survey of Behavioral Models for Social Robots. *Robotics* 8: 54. https://doi.org/10.3390/robotics8030054.

PEPPET, S. R. 2014. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review* 93: 85–176.

https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf (accessed on: 30.07.2021).

PICARD, R. W. 1997. *Affective Computing.* Cambridge (MA, USA).

PRESCOTT, T. J.–ROBILLARD, J. M. 2021. Are Friends Electric? The Benefits and Risks of Human–Robot Relationships. *iScience* 24: 101993. https://doi.org/10.1016/j.isci.2020.101993.

PUSZTAHELYI, R. 2020. Emotional AI and Its Challenges in the Viewpoint of Online Marketing. *Curentul Juridic* 23: 13–31.

RAMIS, S.–BUADES, J. M.–PERALES, F. J. 2020. Using a Social Robot to Evaluate Facial Expressions in the Wild. *Sensors* 20: 6716 (2020). https://doi.org/10.3390/s20236716.

REININGER, A. 2011. *Kempelen Farkas – Wolfgang von Kempelen: életrajz*. Budapest.

RUEBEN, M.–GRIMM, C. M.–BERNIERI, F. J.–SMART, W. D. 2017. A Taxonomy of Privacy Constructs for Privacy-Sensitive Robotics. *arXiv preprint*. arXiv:1701.00841.

SCHEUTZ, M. 2012. The Affect Dilemma for Artificial Agents: Should We Develop Affective Artificial Agents? *IEEE Transactions on Affective Computing* 3: 424–433. https://doi.org/10.1109/T-AFFC.2012.29.

SELBST, A. D.–POWLES, J. 2017. Meaningful Information and the Right to Explanation. *International Data Privacy Law* 7: 237–239. https://doi.org/10.1093/idpl/ipx022.

SØRAA, R. A.–FOSCH-VILLARONGA, E.–QUINTAS, J.–DIAS, J.–TØNDEL, G.–SØRGAARD, J.–NYVOLL, P.–NAP, H. H.–SERRANO, J. A. 2020. Mitigating Isolation and Loneliness with Technology through Emotional Care by Social Robots for Remote Areas. *Mobile Technologies for Delivering Healthcare in Remote, Rural or Developing Regions*. London. https://doi.org/10.1049/PBHE024E_ch16.

SWEENEY, P. 2021. A Fictional Dualism Model of Social Robots. *Ethics and Information Technology* 23: 465–472. https://link.springer.com/article/10.1007/s10676-021-09589-9 (accessed: 30.07.2021). https://doi.org/10.1007/s10676-021-09589-9.

UNICEF 2020. *Policy Guidance on AI for Children*. https://www.unicef.org/globalinsight/media/1171/file/UNICEF-Global-Insight-policy-guidance-AI-children-draft-1.0-2020.pdf (accessed on: 30.07.2021).

WACHTER, S.–MITTELSTADT, B.–FLORIDI, L. 2017. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law* 7: 76–99. https://doi.org/10.1093/idpl/ipx005.

WAINER, J.–FEIL-SEIFER, D. J.–SHELL, DYLAN A.–MATARIC, MAJA J. 2006. The Role of Physical Embodiment in Human–Robot Interaction. *ROMAN 2006 – The 15th IEEE International Symposium on Robot and Human Interactive Communication, 6–8. Sept. 2006*. 117–122. https://doi.org/10.1109/ROMAN.2006.314404.

WINIKOFF, M.–SARDELIĆ, J. 2021. Artificial Intelligence and the Right to Explanation as a Human Right. *IEEE Internet Computing* 25: 116–120. https://doi.org/10.1109/MIC.2020.3045821.