Legal Frame of Non-Social Robots

E. Fosch Villaronga[1]

[1]*Joint International Doctoral (Ph.D.) Degree Erasmus Mundus in Law, Science and Technology coordinated by CIRSFID, University of Bologna, Italy. IDT-UAB, Universitat Autònoma de Barcelona, Spain. e-mail: eduard.fosch@unibo.it*

Abstract. This paper describes some relevant legal aspects concerning non-social robots. Special attention is drawn to Person Carrier Robots (PCaR) and Physical Assistant Robots (PAR). Although concrete legal binding regulations concerning these two sub-types of Personal Care Robots (PCR) are missing, the insertion of this assistive technology into the market arises some legal and ethical concerns. The main concerns include: cognitive aspects involved in the use of the technology; data protection matters: the way roboticists can make their technology comply with to the new European General Data Protection Regulation; liability contexts depending on their degree of autonomy; privacy and autonomy issued; as well as understanding how the decrease in the human-human interaction could undermine the dignity of the person.

Key words: Personal Care Robots, Privacy, Person Carriers, Physical Assistant, Non-Social Robots, Cognitive HRI.

1 Introduction

In 2014, the Industrial Standard Organization released a set of standard safety requirements for Personal Care Robots for the activities of the daily living (ADL). These standard requirements were the first to address non-medical applications of these robots in terms of physical human-robot interaction (HRI). In particular, Personal Care Robots include two non-social robots: Person Carrier (PCaR) and Physical Assistant Robots (PAR); and one social robot: Mobile Servant Robots (MSR) (vid. Fig. 1) [1].

The first two are considered non-social technologies because they do not offer a two-way interaction, they do not express nor understand thoughts or feelings, they are not socially aware, they do not interact unpredictably or spontaneously, and they do not provide the feeling of companionship or of mutual respect [2]. Indeed, non-social robots interact physically with the user, i.e. with a "zero distance between the robot and an object in its external environment" assisting the user to perform tasks, without the need of responding empathically to their users. Non-social robots add only a simple presence to their user's life, and not a sophisticated presence as compared with MSR [3]. Moreover, while non-social robots usually

help the user perform a task (supplementing force, restoring gait or simply conveying them from a place to another one), social robots normally perform tasks *for* the user.

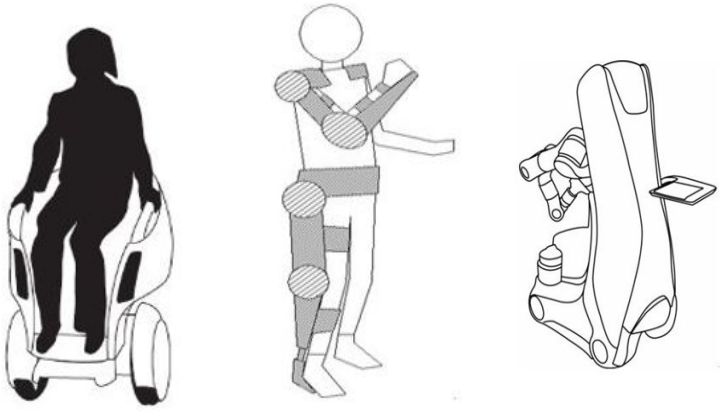

Fig. 1 Non-social and Social Personal Care Robots. Source: ISO 13482:2014 "Robots and Robotics Devices – Safety Requirements for Personal Care Robots.

The HRI also differs within the non-social robots identified by ISO. PAR normally work in a "seamless integration with the user's residual musculoskeletal system and sensory-motor control loops" to assist the user "with minimal cognitive disruption and required compensatory motion" [4]. They are normally fastened to the user's body, although there are restraint-free types. PCaR on the contrary just convey persons to an intended destination and their HRI varies depending on the user interfaces used to estimate the intention of movement.

ISO 13482:2014 addresses the engineering hazards concerning these non-social assistive technology, e.g. robot shape, emissions, electromagnetic interference, robot motion, localization and navigation errors; and also hazards relating to their use, e.g. stress, posture or usage. However, the use of these robots involves other hazards disregarded by the standard such as hazards due to unlawful processing of personal data, incorrect categorization [5], or hazards due to the occurrence of harm or hazards due to the decreased human-human interaction.

This paper addresses legal and ethical concerns regarding the insertion of non-social assistive technology. These concerns include: relevant cognitive aspects involved in the use of the technology; data protection: the way roboticists make their technology comply with the new European General Data Protection Regulation; liability contexts depending on the robot's degree of autonomy; privacy and autonomy matters; and the issue of decreased human-human interaction, which can undermine the dignity of the person.

Four different use cases that will show the urgent need to incorporate other interdisciplinary hazards in industrial standards to address unanswered questions

and protect the final user, which is the ultimate goal for the European Union. Section II will introduce two cases concerning PCaR: (1) the first case concerns data protection issues, mainly cognitive privacy, data portability and profile modules; (2) the second one refers to privacy and security issues in Internet of Things (IoT) environments, and liability in autonomous robots. Section III will include another two cases: (1) the first one will be about data protection, and will focus mainly on consent; and (2) the second one will be about the cognitive aspects of the use of robots, user's autonomy, free will and dignity of the person. Conclusions will be drawn in section IV.

2 Pepa and Her Person Carrier

2.1 Data protection: Data portability

Consider the following use case:

> «Pepa had always problems with her lower-limbs. She is old and she does not like the idea of driving an exoskeleton. The nursing home replaced the old manual wheelchairs with shared person carrier robots. They work in autonomous mode with obstacle recognition through cameras. She uses the carrier when she goes out with her family. The robotic person carrier breaks and she needs a new one, but the producer stopped producing it. Now she will have to use a new one from another producer»

A low-cost wheelchair with a pan-tilt camera inspired this case [6], the article 7 of the European Charter of Fundamental rights [7] and the article 20 of the recently approved General Data Protection Regulation (GDPR) [8].

In theory, privacy is not a major concern for PCaR as their primary use is not related to the invasiveness of the user's private life but rather to convey him/her to an intended destination. Depending on the technology applied to the robot however, this privacy could be undermined. For instance, obstacle recognition through cameras can pose privacy at risk if cameras record other things rather than the obstacles to avoid, especially if the user's private information or the data of third parties are recorded.

The inclusion of person carrier robots available to the different patients in a nursing home also forces the devices to incorporate profile modules so as to identify each user and also to personalize the device (according to the user's preferences). This will raise some privacy concerns. Indeed, the person carrier will:

(1) first need to be protected against vandalism acts and include a password or some bionic identification system to avoid a possible misuse (as ISO 13482:2014 suggests). Attention should be drawn to recent stolen fingerprints in the United States Government [9].
(2) Second, the device should allow data-portability because if it breaks or the producer producing it (as happened with the iBot project) the users should have the possibility to easily transmit setting information and their preferences to a new carrier (it may be possible that when that happens, the user's impairment has worsened and cannot re-train the carrier as previously done with the prior wheelchair). The right to data portability stands for the right of the data subject "to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured and commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided" (*see* Art. 20 GDPR) [8].
(3) Third, all the information collected should be used only for the proper functioning of the device and not for other reasons (e.g. increasing the knowledge of the wheelchair provider to ameliorate the wheelchair, or other business related issues such as: selling new components to compensate some failures, selling some new gadgets to be incorporated to the wheelchair, etc.).

2.2 Internet of Things, Consent and Free Will

Here follows the second case:

> «The new person carrier works in an Internet-of-Thing (IoT) environment. Pepa enjoyed going outdoors with it until she ran over a child accidentally. The mother of the child sued Pepa. Pepa claimed the responsibility was of the nursing home; the nursing home argued in court that it was the carrier's fault because it is autonomous. The manufacturer of it said that the wheelchair works on cloud-robotics base and that, despite being autonomous, once sold to the nursing home it is their responsibility»

This case is inspired by the Dr. Hawking Connected Wheelchair Project [10], a lawsuit for damages caused by an autonomous ground vehicle, and the recent communication from the National Highway Traffic Security Agency (NHTSA) that will interpret the self-driving system of the Google car as the "driver" of it [11].

Although there is no general consensus on the definition, IoT refers to the "scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention" [12]. The infrastructure of IoT challenges the current data protection legislative framework for several reasons. Here are the problems highlighted by the Article 29 Working Party [13]:

- Lack of control and asymmetry: as the processing of the data involved in IoT environments relies on the coordinated intervention of several stakeholders, not only it will be difficult to establish the roles and responsibilities of data controller/processor, but it will also be hard to track the data flows that will be generated. This will entail a complete loss of control from the user as well as a self-exposure of all his/her data.
- Quality of the user's consent. One of the major problems of IoT is the awareness of the user of which objects are processing data from him/her. Classical mechanisms to obtain consent might not apply in this context, as it could be practically impossible to ask for consent each time.
- Inferences derived from data and repurposing of original processing. Modern techniques allow secondary, not pre-specified uses of the collected data very easily, and processing such data with a new aim or for a new use should be considered according to the European Data Protection legal framework.
- Intrusive extraction of behavior patterns and profiling. As this technology is going to be part of the private life of the users (because the wheelchair is used in the nursing home), the possibility to extract behavioral analysis of the collected data now is for real, something which clashes with the principal of data minimization.
- Limitation on the possibility to remain anonymous when using services. Because the idea behind IoT is the personalization of the offered services, it will be very easy to identify the user of a particular technology. Furthermore, "large amount of data processed automatically […] entails a risk of re-identification".
- Security risks: security vs. efficiency. According to the Article 29 Working Party, manufacturers need to balance the implementation of confidentiality, integrity and availability measures at all levels of processing.

IoT combines the possibility to process personal data and also large quantities of sensor data, which can be used further on in "data fusion". The main problem of data fusion is the use of data by third parties and, consequently, the loss of control over that data, both personal and non-personal and the unknown post behavioral analysis of this data [14]. The principle of transparency should play a major role in this data usage. Yet, the intrinsic labyrinthian structure of the data flow between devices, devices and back-end systems, providers and manufacturers, makes

it practically impossible to track data. Tracking data is a key element for accounting reasons (e.g. black boxes) but the more the data collected, the more difficult it is to discover and track its flow [15]. In theory, the data minimization principle (derived from the principle of proportionality of the data processing) has a difficult task. In fact, on the one hand big data techniques are widely available today, on the other hand the intention of data collectors is to process all the available data in the world (e.g. Google's mission for instance is to organize the world's information and make it universally accessible and useful [16]).

All this information processed in data mining can turn into new surveillance options [17], a surveillance that could cause a big brother scenario. In fact, the N=All analysis aims at finding hidden connections that could be possibly useful for future developments [18]. The problem is that "finding the correlation does not retrospectively justify obtaining the data in the first place" [19], especially if there has been no consent for that. On the user's perspective, the use of several IoT connected devices could cause them anxiety [20], although there is no evidence of it yet.

The major problem in any case is similar to what happens in wearable technology, as the "actual customers' perceptions of the benefits are more influential than are their concerns about the risks" [21]. This is caused by a disinformation on the actual risks: first, the providers are more interested in focusing on the benefits rather than on the risks; second, researchers tend to investigate the benefits of a certain technique or device rather than the bad consequences of its use; and third, costumers tend to compare the new device with other, more familiar devices although the latter might differ largely in terms of hardware architecture or functionality. In the end, "when one does not know that one does not know, one thinks one knows" [22].

Concerning the concept of agency, there has been a long discussion on whether machines should or not be granted agenthood. In 2011, Verbeek already considered technology as an active agent [23]; and so did Pagallo when he explained the "digital *peculium*". [24] This Roman legal institution was "the sum of money or property granted by the head of the household to a slave or son-in-power" for the master to avoid further responsibility for his slave's businesses. Pagallo suggests the possibility to apply the same principle in the digital era when we use robots to perform legal transactions. This does not seem that far from reality if we take into consideration that in January 2016 NHTSA stated for the first time in history that driver of the Google car would be the artificial intelligent system.

3 Maria, Peter and the Exoskeletons.

3.1 Data Protection: Consent, Legitimate Purpose.

Consider the following use case:

> « The hospital of Santa Barbara has bought several exoskeletons from the company Exoperfekt S.L. The company sells the device and also offers maintenance and updating services. Every 2 months, the exoskeletons are automatically updated. The Hospital is very happy with the service, as they improve substantially the performance of each device. Users are also very happy. Maria, a patient, feels as if the device knew already her movements»

This case relates to the use of personal data from companies that have already sold their devices to the users, e.g. the case of a smart TV that was processing personal data from the users to ameliorate their system [25]. During a research project, there is normally an ethical committee (Institutional Review Board, IRB) that approves and controls how the collection and processing of personal data is carried out. Once the company has put a device into the market, it is more difficult for an agency to control it (although the Data Protection Agencies are very active on this).

In healthcare domain, the European Union gives special status and stronger protection to health data and considers it as "sensitive data". There there are some relevant considerations to make. First, the collection and processing of personal sensitive data needs to be balanced against other compelling interests (the protection of a person, the invasion of privacy); unequivocal informed consent of the user is needed; and the data collected and processed needs to be proportionate (for the intended task/the purpose which motivated the processing).

Some steps towards the creation of standards to anonymize data have been taken [26], although the anonymisation of data does not involve per se the loss of the "personal" feature of data. In fact, although some companies advocate that only scattered information is processed (normally to escape from the data protection legislation) the Article 29 Working Party already warned that "the processing of that information only makes sense if it allows identification of specific individuals and treat them in a certain way", thus it should be considered as information relating to identifiable individuals [27].

Physical assistant robots are designed to be personal data collectors as they work in a symbiotic manner with their user, despite being in non-medical contexts (as the ISO 13482:2014 pretends). In fact, they are fastened to the user to help a person perform actions according to the user's body characteristics and normal gait. The "household exemption" would not apply because all data is transferred to

many different people (e.g. manufacturers, physicians, etc.) and not for household activities [28].

There are some concerns regarding consent in non-social robots: a) awareness of the processing; b) determining which information should be used for informed consent among special categories of users (elderly people, intellectual disabled people; children, etc.); c) the exact extent to which the user may consent to the processing of data must be unambiguously defined:

a) The principle of fairness requires that the data subject is informed and aware of the data collected. Failing to do so makes the processing unlawful and brings about consequences for the data controllers such as the duty to give compensation to the data subjects, or all the sanctions provided in the national legislations (or any measure in the GDPR).
b) Not only the data subjects need to be aware of the collected data, they also need to give their consent, especially if sensitive data are at stake (as they are regulated more stringently). Of note, informed consent had already some limitations, e.g. language, religious or false expectations [29], and such limitations increase when it comes to the smart devices [30] as the collection of information is not easy to be detected by everyone. The problem is to ensure a meaningful consent in this ubiquitous technology paradigm [31] where users cannot know how their information will be amalgamated or utilized in the future [32] and they need anyway to give their explicit consent [33]. Furthermore, although Art. 8.3 Directive 95/46/EC (still applicable until the GDPR comes into force) states that the prohibition of collective sensitive information "shall not apply where the processing of data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services", these services need to be provided by health professional subjects under national laws, which is not the case when these devices are used for activities of the daily living.
c) The purpose should be "specified, explicit and legitimate". There is an obligation for the data controller to extensively and explicitly describe why and for what purpose the data are being collected, especially if such data can have secondary uses. As the A29WP remarks, either for "raw, extracted or displayed" data, the controllers need to make sure that the used data is compatible with the original consent. If there is the intention to collect data for research, the controller not only needs to say so, he/she needs to have the consent of the user and set down all the appropriate safeguards to cope with that [34].

3.2. Cognitive Aspects, Free Will and Dignity

Here us the last use:

> « Peter on the contrary feels insecure with the exoskeleton. After some time, Peter also realizes the sessions with the therapist reduce. He starts feeling down. One day, tired of living, he decides to fall down the stairs with the exoskeleton. The exoskeleton prevents him from doing so and reports to the doctor this strange behavior»

Subjective perceptions can sometimes constrain the performance of the device, especially in PAR. As PAR work in a symbiotic manner with the user's movement, the users need to feel secure with the device during all gait cycle otherwise they might risk to activate the exoskeleton in an abnormal way [35]. As reported by Salem et al., certified safety and perceived safety are different [36], and this is very important. Although the Personal Care Robot Standard dose hint at the concepts of "mental stress" and "non-contact sensing", however it disregards cognitive aspects. Article 3 EU CFR protects nevertheless both the physical and mental integrity of persons.

Sharkey and Sharkey noticed that one of the problems with assistive technology is the actual replacement of human therapists [37]. Although they referred to assistive technology that monitored elderly people, this also can happen when PAR are introduced in Healthcare facilities, especially if they are used for rehabilitation purposes. The actual use of this technology can reduce the supervision of a human, and this could undermine the dignity of the user.

Some Japanese caregivers have reported something similar. In this case, they were the ones who complained about the insertion of this technology, because "autonomous wheelchair robots might decrease opportunities for rehabilitation". At the same time, they warned that "if seniors become dependent on such a robot and stop moving by themselves, their own physical activity will decrease [38].

The last aspect goes in line with an ethical question yet unsolved: should the robot preserve the human free will or his/her safety? How can the robot be sure that it understands the human commands? Could we talk about of robotic device as an accessory? As the robot capabilities will increase, the more they will have to face ethical dilemmas and the more aware of social norms they will have to be [39].

6 Conclusions

Non-social robots challenge the current legal order regardless of their compliance with current standards. In fact, the current industrial standards disregard sev-

eral interdisciplinary aspects of robot technology that are crucial to offer a complete legal coverage to the citizens.

Future robot technology needs to take into account data protection rules, especially if it will be part of the IoT. In addition, other aspects such as the protection of the second uses of the collected data, informed consent, the legitimate purpose or the new data portability right need to be considered.

Other aspects such as the protection of the mental integrity of the person are going to gain more and more importance with the growing use of Brain-Computer Interfaces. Very soon there will be the need to answer very interesting questions such as "what if your brain reveals important personal information of the user?" In the World Economic Forum in 2016 this question led to a debate where several aspects regarding the intersection of neuroscience and the Law were discussed: from the way neuroscience techniques could be applied to improve the current legal system (to avoid the current existing bias in the decision-making process), to what would happen if a person could use his/her brain to prove his/her alibi [40].

In the end, it is important to start thinking about other sides of robotics and create technology that is safer because, beside traditional safety aspects, other aspects such as privacy, data protection, autonomy and dignity are carefully taken into account. In this way, we will be able to create robots and robotic devices that promote better human-human interaction, which is the final and most important goal.

References

1. ISO 13482:2014 "Robots and Robotics Devices – Safety Requirements for Personal Care Robots
2. Graaf, M. M. A., et al. (2015). What makes robots social?: A user's perspective on character- istics for social human-robot interaction. In Social Robotics (pp. 184-193). Springer Interna- tional Publishing.
3. Sorell, T. and Heather D. (2014) Robot carers, ethics, and older people. Ethics and Information Technology 16.3, pp. 183-195.
4. Tucker et al. (2015) Control Strategies for Active Lower Extremity Prosthetics and Orthotics: A Review. Journal of Neuroengineering and Rehabilitation, 12:1.
5. Fosch-Villaronga, E. (2016) ISO 13482:2014 and Its Confusing Categories. In Wenger et al. (2016) New Trends in Medical and Service Robots. Machine Science, 39.
6. B. K. Kim, H. Tanaka, Y. Sumi, "A Low Cost Robotic Wheelchair System Using a Pan-Tilt Camera and a Visual Marker", Applied Mechanics and Materials, Vols. 789-790, pp. 652-657, 2015
7. Article 7 European Charter of Fundamental Rights, available at: www.europarl.europa.eu/charter/pdf/text_en.pdf
8. European Regulation 2016/679 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).
9. See the BBC (September 2015) Milions of Fingerprints Stolen in the US Government. Available at: www.bbc.com/news/technology-34346802
10. Dr. Hawking Connected Wheelchair Project: www.intel.la/content/www/xl/es/internet-of-things/videos/dr-hawkings-connected-wheelchair-video.html

11. Markoff, J. (2016) Google Car Exposes Regulatory Divide on Computers as Drivers. NY-Times. Available at: www.nytimes.com/2016/02/11/technology/nhtsa-blurs-the-line-between-human-and-computer-drivers.html?_r=0
12. Rose, K., et al. (2015). The internet of things: An overview. The Internet Society (ISOC).
13. Article 29 Working Party (2014) Opinon 8/2014 on the on Recent Developments on the Internet of Things: ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
14. Howard, P. N. (2015). Pax Technica: How the Internet of things may set us free or lock us up. Yale University Press.
15. Medaglia, C. M., and Serbanati, A. (2010). An overview of privacy and security issues in the internet of things. In The Internet of Things (pp. 389-395). Springer New York.
16. Information available at: https://www.google.com/about/company/.
17. Holler, J. et al. (2014). From Machine-to-machine to the Internet of Things: Introduction to a New Age of Intelligence. Academic Press.
18. Mayer-Schoönberger, V, and Cukier, K. (2013) Big data. A revolution that will transform how we live, work and think. John Murray.
19. Information Commisisoner's Office UK (2014) Big Data and Data Protection. Available at ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf.
20. Becker, M. et al (2013) Cyberpsychology, Behavior, and Social Networking, 16(2) pp. 132-135. Available at: online.liebertpub.com/doi/pdf/10.1089/cyber.2012.0291
21. Heetae Y. et al. (2016) User Acceptance on Wearable Devices: An Extended Perspective of Perceived Value. Telematics and Informatics 33, pp. 256-269.
22. Erevelles, S. et al. (2016) Big Data Consumer Analytics and the Transformation of Marketing. Journal of Business Research 69, pp. 897-904.
23. Verbeek, P. P. (2011). Moralizing technology: Understanding and designing the morality of things. University of Chicago Press.
24. Pagallo, U. (2013). The Laws of Robots (Vol. 200). Heidelberg: Springer.
25. BBC (2015) Not in front of the telly: Warning over 'listening' TV. Available at: www.bbc.com/news/technology-31296188
26. Similar to Hamblen M. (2015) UL Creating a Standard for Wearable Privacy and Security. Computerworld. Available at: www.computerworld.com/article/2991331/security/ul-creating-standard-for-wearable-privacy-and-security.html
27. Opinion 04/2007 on the concept of personal data. Article 29 Workin Party. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
28. Article 3(2) of the current Data Protection Directive (95/46/EC) states that the Directive shall not apply to the processing of personal data done by a natural person in the course of a purely personal or household activity. Vid.: ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf
29. Nijhawan, L. P. et al. (2013) Informed Consent: Issues and Challenges. J Adv Pharm Technol Res, 4(3), pp. 134-144.
30. Big Data and Smart Devices and Their Impact on Privacy (2015) DG for Internal Policies. Policy Department. Citizen's Rights and Constitutional Affairs. Available at: www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf
31. Office of the Privacy Commissioner of Canada (OPC) Guidance Documents (2012) Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps. Available at: https://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf
32. Office of the Privacy Commissioner of Canada (OPC) Guidance Documents (2014) Wearable Computing. Challenges and Opportunities for Privacy Protection. Available at: www.priv.gc.ca/information/research-recherche/2014/wc_201401_e.pdf
33. Article 8.2.a) Directive 95/46/CE on the protection of individuals with regard to the processing of personal data and on the free movement of such data

34. Art. 6.1.b) of the EU Data Protection Directive: “further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards”.
35. F. Zhang et al. (2012) Preliminary Study of the Effect of the User Intention Recognition Errors on Volitional Control of Powered Limbs Prostheses. 34th International Conference of the IEEE Engineering in Medicine and Biology Society.
36. Salem M. et al. (2015) Towards Safe and Trustworthy Social Robots: Ethical Challenges and Practical Issues. In: Tapus, A. et al. (eds.) (2015) ICSR, LNAI 9388, pp. 584-593.
37. Sharkey, A., & Sharkey, N. (2012). Granny and the robots: ethical issues in robot care for the elderly. Ethics and Information Technology, 14(1), 27-40.
38. Shiomi M et al (2015) Effectiveness of Social Behaviors for Autonomous Wheelchair Robot to Support Elderly People in Japan. PLoS ONE 10(5), pp. 1-15.
39. Steinert, S. (2014). The Five Robots—A Taxonomy for Roboethics. International Journal of Social Robotics, 6(2), pp. 249-260.
40. World Economic Forum (2016) What if Your Brain Confesses Debate. Available at: www.weforum.org/events/world-economic-forum-annual-meeting-2016/sessions/what-if-your-brain-confesses