Applicability of the GDPR on Personal Household Robots*

*Gizem Gültekin Várkonyi***

Abstract

Recent developments in artificial intelligence (AI) and robotics point to a close future collaboration between humans and machines. Even though the use of personal robots is not yet a phenomenon, findings in technical and legal literature highlight several possible risks inherent in the processing of personal data by such robots. This article contributes to the current discussions on the applicability of the GDPR to AI technologies from three aspects: (i) first, it encourages the use of a scenario method to predict possible future legal problems related to new technologies; (ii) second, it analyzes considerations with the support of the relevant case-law and present comparative expert opinions for overcoming the weak points of the GDPR relevant to AI; (iii) and finally, proposals made in the recommendations part aim to contribute to a better application of the GDPR to AI technologies in personal use.

Keywords: artificial intelligence, robots, personal data, GDPR, scenarios.

1. Introduction

Personal service robots have been purchased in growing numbers since 2018 and purchases are expected to grow at least until 2023.[1] Such robots assist people in various tasks, from entertainment to medical care, offering services to make their life easier. Since the beginning of the COVID-19 pandemic, certain healthcare services have been provided to the patients *via* social robots.[2] In Japan, social robots ease elders' loneliness and provide them several health care services.[3] Even though people do not use household social robots (HSR) yet, their undeniably useful personal services may allow them to enter the most intimate area of individuals, to their households.

* This research was supported by the project No. EFOP-3.6.2-16-2017-00007, titled "Aspects on the development of intelligent, sustainable and inclusive society: social, technological, innovation networks in employment and digital economy". The project has been supported by the European Union, co-financed by the European Social Fund and the budget of Hungary.

** Gizem Gültekin Várkonyi: junior research fellow, University of Szeged.

1 https://ifr.org/ifr-press-releases/news/record-2.7-million-robots-work-in-factories-around-the-globe.

2 *See* at https://spectrum.ieee.org/robotics/medical-robots/how-robots-became-essential-workers-in-the-covid19-response.

3 *See* at www.reuters.com/article/us-japan-ageing-robots-widerimage-idUSKBN1H33AB.

doi: 10.5553/HYIEL/266627012021009001014

Increasing engineering knowledge, accessible low-cost hardware coupled with Big Data bring humanity one step closer to the futuristic image of a life with robots. Machine Learning (ML) techniques have been diversifying with the help of the growing volume of easy-to-access data. Data is the lifeblood of robots since it is both the input and the output of algorithmic assessments in robotic brains (algorithm). For personal service robots this is mainly personal data if the goal is to create personal services.

In the EU, it is the GDPR[4] that provides the framework for the lawful collection and processing of personal data from the individuals. Algorithmic assessments based on personal data challenge the applicability of the GDPR since AI overrides the philosophy of technology neutral enshrined in Recital 15 of the GDPR. It requires stricter regulation on processing personal data by AI. The regulation of AI and robotics has often been discussed by the EU Institutions in the last couple of years. A significant part of the recent legal literature generated by the EU Institutions – much in line with the points summarized under the literature review title of this work – show that risks arising from AI technologies, need better regulation. Data protection has always been included in these documents, even though a few works exist that evaluate the risks specific to the right to data protection in AI technologies. Risks regarding the possible invalid consent practices, transparency, difficulties in providing sufficient information on these technologies, and the ethical aspects have been mentioned repeatedly in such works.[5] In order to foresee the challenges faced when designing data protection law of the EU for AI and robotics, this work introduces a scenario method that was constructed on a comprehensive literature analysis specific to AI and the law. The literature review lays down the main hypotheses of the research which are tested through the analysis of the GDPR and the CJEU case-law harmonized with the author's opinions. Expert opinions that were collected by interviews, helped conducting a comparative analysis among four EU MS's and mostly served to support the analysis conducted by the author. Finally, the solutions offered by the article may support the application of the GDPR in the AI technologies.

4 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, GDPR).

5 White Paper On Artificial Intelligence – A European Approach to Excellence and Trust, COM(2020) 65 final; Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, SWD (2018) 137 final; *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on Artificial Intelligence, April 2019; Giovanni Sartor, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, Panel for the Future of Science and Technology; Aimee van Wysenberg, *Artificial Intelligence: From Ethics to Policy*, EPRS Study Panel for the Future of Science and Technology, June 2020.

doi: 10.5553/HYIEL/266627012021009001014

2. Literature Review

An initial note should be made about the terminology used in the entire work. This work uses the term robot interchangeably with AI, since this approach is visible in the technical foundations of the terms, as well as in their relations with law.[6] Robots are specifically chosen, since their physical representativeness in real world make them more intelligent and to be perceived more real.[7] The physical appearance shows significant difference between the social bots and social robots,[8] especially in legal research.[9] *Social robots*, that are able to socially interact with people[10] like another human, might cause more privacy infringements than a social bot. The hardware capabilities of robots, such as sensors, cameras, microphones, and a variety of actuators assist them to collect more data about the real world, including personal data, as it will be discussed below.

2.1. Technical Considerations

The brain of the AI systems, the algorithm is developed with the help of ML techniques that have a crucial impact on collecting and processing (personal) data. Data is actually the lifeblood of robots because a typical ML lifecycle starts with data collection[11] and continues with an endless data evaluation and data generation.

First, the robot's physical advantage, then the humanoid appearance and behavior combined with the natural language interactions causing *Uncanny Valley* encourage people to disclose more personal data to a robot. The term Uncanny Valley was created by the (social) roboticist Masahiro Mori,[12] and was used for

6 Robin R. Murphy, *Introduction to AI Robotics*, MIT Press, Cambridge, US, 2001, p. 248; Xiuquan Li & Hongling Jiang, 'Artificial Intelligence Technology and Engineering Applications', *Applied Computational Electromagnetics Society Journal*, Vol. 32, Issue 5, May 2017, p. 381; *A Definition of AI: Main Capabilities and Scientific Disciplines*, High-Level Expert Group on Artificial Intelligence, April 2019; ISO 8373:2012(en) Robots and Robotic Devices – Vocabulary, para 2.6.

7 Christophe Leroux *et al.*, *Suggestion for a Green Paper on Legal Issues in Robotics*, euRobotics – The European Robotics Coordination Action, 7th Framework Programme, 2012, p. 60.

8 Oliver Korn *et al.*, 'Perspectives on Social Robots: From the Historic Background to an Experts' View on Future Developments', *Proceedings of the 11th PErvasive Technologies Related to Assistive Environments Conference*, PETRA '18, New York, NY, USA: ACM, 2018, p.188; *Draft Motion for a Resolution on Automated Decision-Making Processes: Ensuring Consumer Protection, and Free Movement of Goods and Services*, European Parliament, Committee on the Internal Market and Consumer Protection, 2019/2915(RSP), 21 January 2020, p.3, para D.

9 Carolina Alves de Lima Salge & Nicholas Berente, 'Is That Social Bot Behaving Unethically?', *Commun. ACM*, 60, 2017, p. 30.

10 Terrence Fong *et al.*, 'A Survey of Socially Interactive Robots', *Robotics and Autonomous Systems*, Vol. 42, 2003, p. 145; Eduardo Fosch-Villaronga, *Towards a Legal and Ethical Framework for Personal Care Robots: Analysis of Person Carrier Physical Assistant and Mobile Servant Robots*, Doctoral dissertation, Erasmus Mundus in Law, Science and Technology Consortium, 2017, p. 52; Cynthia Breazeal, *Designing Sociable Robots*, MIT Press, Cambridge, US, 2002.

11 Harini Suresh & John V. Guttag, 'A Framework for Understanding Unintended Consequences of Machine Learning', *ArXiv Preprint ArXiv:1901.10002*, 2019.

12 *The Uncanny Valley: The Original Essay by Masahiro Mori*, translated by Karl F. MacDorman & Norri Kageki, IEEE Spectrum, at https://spectrum.ieee.org/automaton/robotics/humanoids/the-uncanny-valley.

doi: 10.5553/HYIEL/266627012021009001014

the first time in his Japanese publication about forty years ago. Mori made a strong relationship between the human deception and the mathematical functions (when the value x increases, the equivalent y also increases) and conceptualize the deception in the case of robots in a way that, "in climbing toward the goal of making robots appear human, our affinity for them increases until we come to a valley". More precisely, as long as the robots will be designed in a way they look or act like human (f(x)), people will start to have feelings (*e.g.* affection) towards robots (y) and therefore not considering them as machines. As the humanoid design increases, so will the humanoid perception of robots (f(x)=y). Personalization of robots through RL techniques, on the other hand, directly affects people's perception of a (social) robot; the more human the robot is, the user's perception of humanoid companion increases. This kind of perception might manipulate people emotionally, hence, people may even assume that a robot also has emotions deceiving the user.[13] The emotional engagement with robots encourages people to disclose more personal information for functional rewards. When these functional personalized rewards are combined with a humanoid outlook, people tend to engage with robots more, falsely thinking that robots are human, because they act and look like humans.[14] People living with social robots are be required to share personal data if they wish to receive personalized services, however, illusionary perception of the robot in people's minds might raise risks towards the right to data protection. Obviously, more uncanny valley strengthens the trust of people in robots which, in the end, causes even more data disclosure.

In addition to the design factor, and even more significantly, *the nature of the ML techniques which require constant data collection make robots unpredictable data collection by design*. The algorithm then learns to create its own decision-making rules unlikely to the classic programs, where the rules are pre-defined.[15] Once the personal aspects of an individual are evaluated by an algorithm, the output on that individual becomes a new personal data. Even if the collected data is not personal, big data and ML techniques easily turn it to personal data.[16]

The data collection by AI systems is unpredictable, and so is the output of the conducted process on the data. The term *Unpredictable by Design*[17] refers to the fact that robots constantly acquire new data that they feed the algorithm with and generating outputs that are almost impossible to foresee at the beginning of

13 Pauline Kuss & Ronald Leenes, 'The Ghost in the Machine – Emotionally Intelligent Conversational Agents and the Failure to Regulate 'Deception by Design' *SCRIPTed*, Vol. 17, Issue 2, 2020.

14 Anja Richert *et al.*, 'Anthropomorphism in Social Robotics: Empirical Results on Human-Robot Interaction in Hybrid Production Workplaces', *AI & SOCIETY*, Vol. 33, 2018, p. 420.

15 Christian Sandvig *et al.*, 'Automation, Algorithms, and Politics – When the Algorithm Itself Is a Racist: Diagnosing Ethical Harm in the Basic Components of Software', *International Journal of Communication*, Vol. 10, 2016, p. 4978.

16 Michael Veale *et al.*, 'Algorithms That Remember: Model Inversion Attacks and Data Protection Law', *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Vol. 376, 2018, p. 2.

17 Jason Millar & Ian Kerr, 'Delegation, Relinquishment, and Responsibility: The Prospect of Expert Robots', *in* Ryan Calo *et al.* (eds.), *Robot Law*, Edward Elgar Publishing, Cheltenham, 2016.

doi: 10.5553/HYIEL/266627012021009001014

the whole processing activity. Statistical and mathematical calculations applied on a vast amount of data through the algorithms developed with unsupervised ML have become more complex and more unpredictable.[18] Indeed, such outputs are personal outputs,[19] either being the input personal data or not, since the functionality of the robot is for personal use. Social robots could reach more accurate results of the user's personality over time and with the help of ML techniques that offer more personalized services.[20] Closely related to this concept, these outputs could be used for new purposes that are different from the initial ones[21] or serve to new purposes that the data controller wishes to benefit from.[22] A separate question is whether algorithmically generated personal data fall under the GDPR's scope, and processing personal data by robotic brains is not allowed, unless the data subject gives a (valid) consent.

One of the goals behind the human-AI collaboration is to reduce human involvement with the repetitive and machine-learnable tasks, therefore, to enable robots to act autonomously in real life. Depending on the ML technique used for the development of a social robot, their autonomous nature raises some questions about liability like who is liable in case a robot causes an undesired situation. Even though different discussions on robot liability have already been heard,[23] the situation draws a complex picture of data protection, since there could be many actors involved in data processing, like developers, hardware

18 Woodrow Barfield, 'Liability for Autonomous and Artificially Intelligent Robots', *Paladyn, Journal of Behavioral Robotics*, Vol. 9, Issue 1, 2018, p. 196; Andreas Matthias, 'The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata', *Ethics and Information Technology*, Vol. 6, Issue 3, 2004, p. 171; Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Establishing the Digital Europe Programme for the Period 2021-2027, SWD(2018) 305 final, p. 5; Kaori Ishii, 'Comparative Legal Study on Privacy and Personal Data Protection for Robots Equipped with Artificial Intelligence: Looking at Functional and Technological Aspects', *AI & Society*, Vol. 3, Issue 4, 2019, p. 512.

19 Martijn van Otterlo, 'Gatekeeping Algorithms with Human Ethical Bias: The Ethics of Algorithms in Archives, Libraries and Societty', *ArXiv Preprint ArXiv:1801.01705*, 2018, p. 28.

20 Wu Youyou *et al*., 'Computer-Based Personality Judgments Are More Accurate than Those Made by Humans', *Proceedings of the National Academy of Sciences*, Vol. 112, Issue 4, 2015, p. 1038; Anthony G. Francis Jr. & Thor Lewis, 'Methods and systems for robot personality development', U.S. Patent 8996 429 B1, 31 March 2015.

21 Guidelines 05/2020 on consent under Regulation 2016/679, European Data Protection Board, 4 May 2020, para. 56.

22 Bart Custers & Helena Uršič, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection', *International Data Privacy Law*, Vol. 6, Issue 1, 2016; Nicola Jentzsch, *Financial Privacy: An International Comparison of Credit Reporting Systems*, Springer, Berlin, 2007, p. 39; Tijmen Wisman, 'Purpose and Function Creep by Design: Transforming the Face of Surveillance Through the Internet of Things', *European Journal of Law and Technology*, Vol. 4, Issue 2, 2013.

23 Gabriel Hallevy, 'The Criminal Liability of Artificial Intelligence Entities-From Science Fiction to Legal Social Control', *Akron Intellectual Property Journal*, Vol. 4, Issue 2, 2010; Peter M. Asaro, 'Robots and Responsibility from a Legal Perspective'. *Proceedings of the IEEE*, Vol. 4, Issue 14, 2007; Susanne Beck, 'The Problem of Ascribing Legal Responsibility in the Case of Robotics', *AI & Society*, Vol. 31, 2016; Robert van den Hoven van Genderen, 'Do We Need New Legal Personhood in the Age of Robots and AI?', *in* Marcelo Corrales *et al*. (eds.), *Robotics, AI and the Future of Law*, Springer, Singapore, 2018; Barfield 2018.

doi: 10.5553/HYIEL/266627012021009001014

providers, or even the users.[24] At this point, it is legitimate to ask, "who is the data controller for an autonomous machine with self-learning capabilities?"[25]

Lastly, the ongoing discussions about the *black-box*[26] algorithms referring to the difficulty in providing explanations on the outputs that the algorithms reach would consist of the final consideration under this title. However, this work does not look into the technical details of the problem, it rather focuses on the effect of the complexity of the technology on average users to perform informed choices based on information provided them.[27] This topic will be later raised under the practical considerations title.

2.2. Legal Considerations

In light of the technical considerations, it is possible to identify the legal problems while examining the application of the GDPR focusing on the consent, purpose limitation, fulfillment of the information obligation and the liability issues.

Initially, as the unpredictable data collection by design concept showed, a social robot placed at the households would be constantly profiling the data subjects. Article 22 GDPR entrusts data subjects the "right to not to be subject to a decision based solely on automated processing, including profiling" unless such a decision is legally permitted, like an explicit consent. In line with Article 7 of the GDPR, the consent should be valid, if it is specific, freely given, informed, and indicated with a clear affirmative action or a statement by which data subject give permission that their data is processed. In order a consent to be considered specific, the purpose(s) of data processing should be clearly defined, and the data subjects shall be informed about these purposes by the data controller. In order a consent to be considered freely given, broadly, data subjects should be provided with a concept leading them to assess the possible risks raised by the data processing activity. Further, data subjects shall be provided sufficient information in line with the rules stipulated in Articles 12 and 13 of the GDPR. Article 12 sets forth the rule on the information to be "concise, transparent, intelligible and easily accessible form, using clear and plain language". Article 13

24 European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL); Sartor 2020.

25 Artificial Intelligence, Robotics, Privacy and Data Protection. Room Document for the 38th International Conference of Data Protection and Privacy Commissioners, European Data Protection Supervisor, October 2016, p. 9.

26 Sandra Wachter *et al.*, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law*, Vol. 7, 2017, p. 78; Nizan Packin & Yafit Lev-Aretz, 'Learning Algorithms and Discrimination', *in* Woodrow Barfield & Ugo Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing, Cheltenham, 2018, p. 5; Ronald Yu & Gabriele Spina Alì, 'What's Inside the Black Box? AI Challenges for Lawyers and Researchers', *Legal Information Management*, Vol. 19, 2019; Oscar Li *et al.*, 'Deep Learning for Case-Based Reasoning through Prototypes: A Neural Network That Explains Its Predictions', *Proceedings of the AAAI Conference on Artificial Intelligence*, 2018, p. xxxii; *AI in the UK: Ready, Willing and Able?*, House of Lords Select Committee on Artificial Intelligence, Report of Session 2017-19, London, 16 April 2018, p. 95.

27 Van Wysenberg 2020.

doi: 10.5553/HYIEL/266627012021009001014

of the GDPR lists the information that shall be provided by data controllers to be able to fulfill their informing obligation such as giving information on the data controller's identity, contact information, purposes, data transfers to third parties, and other similar basic information.

As a result of the new outputs that were unpredictably generated by AI, the probability of using the data in a multi-purpose manner arises. It might not always be possible to simply create a list of clear purposes of data processing, even though a solution could be to ask for a new consent each time there is a new purpose. Once the decision (the output) has been made by the system, the purpose simply was already born, meaning that the data subject is basically not in a position to exercise its right to contest against being subjected to an algorithmic decision making (ADM), but only to give permission to that new purpose. Such re-purposing[28] is a result of the nature of AI but is absolutely not permissible by the GDPR. If there is no specific purpose, there can be no valid consent.[29]

Returning to the Uncanny Valley effect and to the personalization concept, these concepts directly affect the people's free will, because the more humanoid the robot is, the more user's free will is manipulated. This may be an emotional manipulation; hence, people might even assume that a robot can develop emotions towards them,[30] so they interact with the robots without thinking of the privacy borders. For example, this humanoid effect creates a feeling of empathy[31] towards a machine, so the services they benefit from are maximized,[32] which is illusionary in people's minds. Obviously, the more the Uncanny Valley increases the trust of people towards robots, leads to more shared data without a valid consent.[33]

Referring to the explainability concept, this work builds a bridge between the consent and the purpose of limitation principles, and state that pre and/or post

28 Custers & Uršič 2016.

29 *Scientific Foresight Study Ethical Aspects of Cyber-Physical Systems*, European Parliament, Science and Technology Options Assessment Panel, June 2016, pp.7-10. European Parliament Resolution of 12 February 2019 on a Comprehensive European Industrial Policy on Artificial Intelligence and Robotics, 2018/2088(INI), para. 128; Zrinjika Dolic *et al*., *Robots in Healthcare: A Solution or a Problem?*, Study for the Committee on Environment, Public Health, and Food Safety, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, p. 8; Giovanni Sartor, *New Aspects and Challenges in Consumer Protection. Digital Services and Artificial Intelligence*, Study for the Committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, European Parliament, 2020; van Wynsbergh 2020.

30 Kate Darling, '"Who's Johnny?" Anthropomorphic Framing in Human-Robot Interaction, Integration, and Policy', *in* Patrick Lin *et al*. (eds.), *Robot Ethics 2.0*, Oxford University Press, New York, 2017; Robert van den Hoven van Genderen, 'Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics', *European Data Protection Law*, Vol. 3, Issue 3, 2017.

31 Fosch-Villaronga 2017, p. 254.

32 Maartje de Graaf, 'An Ethical Evaluation of Human–Robot Relationships', *International Journal of Social Robotics*, Vol. 8, Issue 4, 2016, p. 590.

33 David Leslie, *Understanding Artificial Intelligence Ethics and Safety: A Guide for the Responsible Design and Implementation of AI Systems in the Public Sector*, The Alan Turing Institute, 2019, p. 5.

doi: 10.5553/HYIEL/266627012021009001014

explanations[34] – that are generic to the average user – do not make sense, since the GDPR does not explicitly regulate the information and explanation to be provided to the data subjects in case an ADM is involved.[35] In a digital world where people do not often read or understand the privacy and consent statements that are under dynamic change constantly,[36] giving a valid consent is nothing more than just an imagination. Specific to the AI, where an algorithmic decision carries a certain degree of autonomy, the risk of rendering AI's action becomes unexplainable.[37]

The final topic to be evaluated under this title is an inspiration from the discussions on the possible liability issues in case an autonomous robot causes invalid consent practices. Combining also with the cultural-philosophical narratives that data controllers may carry,[38] it is hard to identify the exact data controllers (also the data processors that are left out of the scope of this work to keep simplicity) that should provide the consent forms and the information to the data subjects will be analyzed in the further sections.

2.3. Practical Considerations

Based on the technical and legal considerations discussed above, there are questions raised about the applicability of the GDPR on HSR from the practical considerations point of view. Besides the technical aspects of AI systems where the possibility of obtaining consent and providing right information about the purposes is reduced, the GDPR, practically, does not oblige the data controllers to ensure the understandability of the information they provide, rather to provide information that is generic to all data subjects.[39] Even though several guidelines build a framework of the concept of the understandable information[40] (meaningful and intelligible information) the term refers to the average data subjects' level of understanding, without requiring a strict analysis on the individual information needs. The data subject specific conditions in terms of

34 Amina Adadi & Mohammed Berrada, 'Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)', *IEEE Access*, Vol. 6, 2018; Wachter *et al*. 2017.

35 Gizem Gültekin-Várkonyi, 'Operability of the GDPR's Consent Rule in Intelligent Systems: Evaluating the Transparency Rule and the Right to Be Forgotten', *in* Andrés Muñoz *et al*. (eds), *Intelligent Environments*, IOS Press, 2019.

36 Jakub Míšek, 'Consent to Personal Data Processing – The Panacea or the Dead End', *Masaryk University Journal of Law and Technology*, Vol. 8, Issue 1, 2014, p. 76; Bart Custers *et al*., 'Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law'. *SCRIPTed: A Journal of Law, Technology and Society*, Vol. 10, 2013, p. 440; Philip Boucher, *Artificial Intelligence: How Does it Work, Why Does it Matter, and What Can We Do about It?*, European Parliamentary Research Service Scientific Foresight Unit, PE 634.421, 2019, p. 15.

37 EP 2017, para. AI.

38 Krisztina Karsai, 'Algorithmic Decision Making and Issues of Criminal Justice – A General Approach', *in* Cristian Dumitru Mihes (ed.), *In Honorem Valentin Mirişan*, Universul Juridic SRL., 2020, pp. 146-161.

39 Tim Miller, 'Explanation in Artificial Intelligence: Insights from the Social Sciences', *Artificial Intelligence*, Vol. 267, 2019, p. 4; Gültekin Várkonyi 2019.

40 Article 29 Working Party, 'Guidelines on Consent under Regulation 2016/679', p. 7; Judgment of 17 July 2014, *Joined Cases C-141/12 and C-372/12, Y.S.*, ECLI:EU:C:2014:2081, para. 57.

doi: 10.5553/HYIEL/266627012021009001014

providing either in case of providing pre or post explanations are left out of the GDPR.[41]

The problem with the *GDPR's unclear statements on providing understandable information to the data subjects* belonging to vulnerable groups (except Article 8 GDPR proclaiming child consent rules) could be raised here as an example. HSR services will most probably be available first to the people who need support with their health or social conditions. One of the results of the Explain project points that 95% accurate decisions may prevail over the importance of the right to explanation in the case of health,[42] meaning that patients might give up their right to explanation in return of receiving a better health care. The elderly might be considered fragile since they could be more open to emotional manipulation and deception.[43] Even though such engagement is desirable and possible,[44] their free will is compromised.[45] People with disabilities is another group that was left out of the understandable information concept, and who might be both in physical and psychological contact with HSR. There is need in informing people that belong to such categories (which the algorithms have already created) with special attention, rather than applying the average user concept to them.

As a result of the previous analysis, *three hypotheses will be further tested* in this work: *(i)* H1: ML techniques enabling AI technologies to perform autonomous decisions, together with profiling, might cause extraction of new data about the data subjects, which is contrary to the principles put forth in the GDPR. *(ii)* H2: Data repurposing, unforeseeable data collection and system functionality, transparency and explainability problems, and complexity in identifying data controllers may cause ineffective consent applications. *(iii)* H3: Unclear legal rules on advanced technologies may hinder the understanding of individuals about the functionality of such technologies; therefore reduces the better enforcement of the legal rules.

3. Methodology

The methodology chosen for testing the hypotheses is the *scenario method* that belongs to the Futures Research Methodology[46] family. Scenarios have been used for forecasting by policy analysis researchers for more than 60 years, with the aim of connecting present issues with the future through cause and effect links.[47] The intention behind the scenarios is to assist policymakers to act now instead of acting later in the emergency cases. A similar goal was already adopted in this

41 Sartor 2020, p. 63.

42 *Project explAIn: Interim report*, Information Commissioner's Office, 2019, p. 15.

43 Tobias Körtner, 'Ethical Challenges in the Use of Social Service Robots for Elderly People', *Zeitschrift für Gerontologie und Geriatrie*, Vol. 4, 2016, p. 305.

44 Panagiotis Tzirakis *et al.*, 'End-to-End Multimodal Emotion Recognition Using Deep Neural Networks', *IEEE Journal of Selected Topics in Signal Processing*, Vol. 11, Issue 8, 2017, p. 1305.

45 EDPB, para 24.

46 Jerome C. Glenn & Theodore J. Gordon, *Futures Research Methodology*, Version 3.0, The Millennium Project; 3.0 edition, 2009, Scenarios section.

47 Id. p. 5.

doi: 10.5553/HYIEL/266627012021009001014

work; to provide some inputs for the EU lawmakers who have been working hard on shaping the future of data protection legislation facing the challenges caused by the AI technologies of today and the future.

Scenario method, together with other forecasting methods, is being practiced in the field of law and technology by many scholars. The Millennium Project,[48] in which all the methodologies have been used for forecasting several issues, including the legal ones, is the most comprehensive work in this sense. Specific to the law and robotics, there are examples of practicing the method in different intersections. It might seem small in quantity, but they give enough background information to understand the applicability of the methods in this field. Dark scenarios designed for helping to identify the impact of AI technologies on data protection,[49] a short scenario questioning and analyzing the liability of robots,[50] scenarios focusing on assessing the ethical and practical aspects of autonomous robots[51] were all created and used for suggesting better policy options for the policymakers. Finally, Ballard and Calo's draft work[52] presented in the WeRobot 2019 conference was the driving force of choosing the present work's methodology, since it was focusing directly on Robolaw with the aim of preventing unintended consequences of future legal problems with the help of a foreword thinking way. Futures research methods could offer efficiency in identifying and raising solutions towards the problems of legal aspects of emerging technologies as proven in the literature.[53]

The scenario constructed in this work is *a result of a comprehensive technical and legal analysis*, as well as based on personal experiences gained from the Sci-Fi and legal literature. Analysis of the scenario firstly considered under personal interpretations in light of the GDPR, the case-law of the CJEU and the literature. Then, with the hope for identifying new interpretations, expert interviews were collected. Such a method is often being used in legal sciences[54] with the same purposes. The interviews were conducted altogether with 15 experts from four EU Member States, specifically, from Finland, Hungary, Italy, and the Netherlands. These countries were chosen based on their geographical representation, meaning that the design of this work chose a sample from the Central and Eastern, Northern, Southern, and Western European States. Furthermore, these countries' rank in the AI readiness Index was considered as

48 *See* at www.millennium-project.org.

49 Pasi Ahonen *et al.*, 'Dark Scenarios BT', *in* David Wright *et al.* (eds.), *Safeguards in a World of Ambient Intelligence*, Springer Netherlands, Dordrecht, 2008.

50 Christina Mulligan, 'Revenge against Robots', *South Carolina Law Review*, Vol. 69, Issue 3, 2018.

51 Henrik Carlsen *et al.*, 'Co-Evolutionary Scenarios for Creative Prototyping of Future Robot Systems for Civil Protection', *Technological Forecasting and Social Change*, Vol. 84, 2014.

52 Stephanie Ballard & Ryan Calo, *Taking Futures Seriously: Forecasting as Method in Robotics Law and Policy*, We Robot 2019 (draft), p. 3.

53 In his work, Minkkinen proposed a new futuristic privacy model shaped by an institutional approach which should be based on the dynamics in understanding the privacy and historical processes. Matti Minkkinen, 'Futures of Privacy Protection: A Framework for Creating Scenarios of Institutional Change', *Futures*, Vol. 73, 2015.

54 Dawn Watkins & Mandy Burton, *Research Methods in Law*, Routledge, London, 2013.

doi: 10.5553/HYIEL/266627012021009001014

the second criteria.[55] Since the GDPR is a regulation and should be applied in every EU MS in the same way, there was no other criteria defined for the sampling method. Choosing the experts (sampling) was based on the following criteria: the Expert has to be working at a law firm or an institution dealing with the interpretation or implementation of the GDPR; they must have a professional interest in AI technologies (*e.g.* published a paper, gave a lecture, analyzed a legal case); and has to accept to be a part of the interview. The questions of the interview were sent to the experts beforehand, leaving some time for the experts to carefully read and pose their questions in lack of clarity.

4. The Scenario: Introduction

This is the future where humans became more dependent on technology. Autonomous cars replaced public transportation and reduced personal cars in traffic; drone delivery replaced the traditional door to door delivery services. Waste disposal robots sweep the streets all day with a smiling face, food and drinks are served at the hands of robo-waiters in cafés. Human beings spend more time developing their personal selves and developing and using technology for their own good.

This is the age of technology in which the cost of hardware and software requirements for producing not just a single robot, but dozens. Most of the people in Europe can easily afford a personal service robot enhanced with several ML techniques. These robots are the so-called *Social Robots* that can enter into social interactions with human users to serve them in different fields, starting from maintaining the home to providing health care services (also in the private home). Depending on their level of AI, these robots can fulfill single to multiple tasks for personal use. For this reason, they are also called as personal household social robots. These multi-purpose robots are very popular since they offer tailor-made services for anyone who opts in sharing their personal life with them. Their humanoid specifications and features make the user feel comfortable during their interactions, which makes it easier for the robots to collect necessary data to develop their algorithms to the personal satisfaction of the user. Companies (the entities producing, selling, and maintaining the robots, and dealing with few problems arising from personal use) behind these robots ensure a high level of security and abide by the strict principle of no-surveillance by third parties and are operating the robots in a safe and trustworthy way. The machines can make highly accurate and bias-free decisions, thanks to the ML research and technology investments made in this field a decade ago.

4.1. Life with a Social Robot at Home

Julia is a successful businessperson in her early forties living alone since she and her husband got divorced two years ago. She has a son whom she meets quite often in a week. Since she works more than a usual after she got divorced, she

55 *See* at www.oxfordinsights.com/government-ai-readiness-index-2020.

doi: 10.5553/HYIEL/266627012021009001014

realized that she could replace some of the repetitive household work with a robot and share her loneliness with it, just like her colleagues did so. She purchased the personal HSR called Robinsan,[56] a Social Robot, whose algorithms run based on and defined by the objective of "maintaining and optimizing the well-being of people". It is able to complete several tasks related to home maintenance and personal care, from cleaning to ordering food, from home security to entertainment, *etc*., based on the service module the user subscribes. Robinsan's algorithm runs several applications in one central cloud-based database owned and operated by the Company selling it.

Julia evaluated the first month with Robinsan as 'very efficient' due to the robot's high level of performance in completing the tasks she assigned to it. She decided to go on with Robinsan by notifying the Company and upon that, the Company mentioned some of the other functions of the HSR, such as personalized health-care assistance.

A couple of months later, Julia was informed that she has early onset Alzheimer's disease (AD). She already received treatment from her doctor, but she believes in the benefit of a supportive treatment besides the medical one on reducing the AD's effects. Such a supportive treatment can be, for example, daily activities improving her cognitive skills (memory), or herbal tablets based on her physical and psychological needs.[57] She remembers the information given by the Company regarding Robinsan's function as a personal health care assistant and she decides to extend her subscription to the basic personal health-care module which then could be specially tailored to her specific disease. Since it is a matter of her health, she did not much care about all the informative documents and consent papers that the Company made her sign, she took a quick look at them upon purchase.

4.2. Operating the Social Robot

While the installation was on-going, Julia felt exhausted with many interruptions during her interactions with Robinsan, as consent panels were embedded in the installation process to fulfill the Company's relevant obligations. She paid attention to the consent statements several times but did not understand why all these repetitive information (name of the data controller, address, data processing purposes, *etc*.) was presented each time. She also did not understand some of the statements, thinking they were too technical for her. Once Robinsan was updated with the new health-care functionality, she could then start uploading all personal information regarding her health status, by scanning the papers, or by oral introduction. Besides Robinsan collecting data such as pulse, blood pressure, sweat concentration, hemoglobin saturation, *etc*., through a chip (owned only by the Company) embedded in Julia's arm, it could also analyze

56 This name consists of two words which one of them is robot and the other is 'insan' meaning human in Turkish.

57 The idea of core genomic medicine targeting to deliver personalized medicines and treatments to the patients by analyzing their genomic data (*e.g.* DNA) is based on *Genomics and Genome Editing in the NHS*, House of Common Science and Technology Committee, 2018.

doi: 10.5553/HYIEL/266627012021009001014

physical indicators such as fatigue, happiness, depression, dizziness, *etc.*, *via* Facial Recognition, without needing the chip.

By that time, Robinsan became an important part of Julia's life. She trusted the robot and let it move freely at home without territorial restrictions. She had no fear to share her personal issues with Robinsan since she felt like it was human, due to its humanoid behavior. Whenever Julia felt sad, Robinsan could detect it and cheer her up with several personalized services, such as, playing her favorite song or talking with her. She interacted with Robinsan every day, disclosed her feelings and opinions, and she actually was no longer lonely in this way. She finally decided to approve all the consent statements delivered by the Company and Robinsan's user interface without giving them a further thought.

As part of the health care function, Julia taught the robot to prepare her medicines and bring them every day at a certain time. She also taught Robinsan to order her medication whenever it ran out and to make her recommendations on OTC, holistic herbal medicines if the robot thought those could be helpful for her. Robinsan decides about the additional medication based on Julia's monthly health status evaluation compiled from several resources such as data describing her physiological and emotional status.

Robinsan also prepares personalized memory training exercises based on Julia's own settings. It can present slices of videos and pictures from the events which Julia can decide about and 'teach' the robot. Robinsan could keep records of particular family activities through videos or pictures, which could then be presented in a gamified way to make her engage more with the activity. Robinsan's algorithm chooses the most important moments such as when she is happy, as well as important events such as birthdays, name days, and so on. It could then project the pictures or videos on flat surfaces or displays them on its small touchscreen or using the smartphone Julia has to display them. Besides voice and face recognition and natural language processing, the HSR could analyze mimes and emotions of people, so it could decide on at what confidence interval Julia might remember a certain moment. Julia taught the robot to choose some moments from her daily activities, including when her son visited her. She already asked her son's consent for being part of such recording, and naturally, he did not receive a negative answer. After the recording was finished, Robinsan shared the files with them.

4.3. Problem Statement

After the HSR ordered the second refill for Julia's prescription medication, she opened the delivery box and found her medicines, a box of herbal vitamins, and a leaflet introducing a non-clinical treatment for drug addiction. She discussed the leaflet with her son, since he was the only one who interacted with Robinsan, and who immediately looked for an explanation for the leaflet in Robinsan's operating system. Besides very basic information such as a non-exhaustive list of data Robinsan used for prediction, they found some technical information that they could not understand much. Her son sent an e-mail to the Company requesting an explanation, and the Company responded explaining that personal data might be collected in the course of ordering food, or while preparing for the memory

doi: 10.5553/HYIEL/266627012021009001014

exercise, from both of them (Julia and her son) during their interactions with the HSR. The Company claimed that the information on the decision-making procedure of Robinsan was already explained in an easy-to-understand way to the general public. Furthermore, the Company delivered a report revealing the 85% probability of drug usage by the data subject (in the form of anonymized data).[58] The Company indicated that it was Julia who purchased Robinsan and allowed it to collect data, therefore the means and purposes of data collection were communicated to her. Finally, the Company pointed out the notification which simply informed the users of the risk of having Robinsan at home, generating unpredictable results. The National Supervisory Authority is now preparing for an investigation, with several questions in the case file.

5. Evaluation of the Scenario

5.1. Part I. Case-Law Analysis

Based on the problems stated, first the liability issue will be analyzed in light of the household exemption, then the question of consent and the data controller's information obligations will follow in the course of analysis. Obviously, the main responsibility always belongs to the legal person(s) as a data controller, a different approach is taken into account in this work that is questioning the probability of the partial responsibility of the natural person that is the main user and the data subject. Such a probability was born in light of the existed case-law, that will be presented below. These cases posed the question whether using new technologies for in-house personal purposes should be considered as a household activity. Even though the answer to the question may not always be disputable, the aim here is to make a slight connection between the question of consent and responsibility.

5.1.1. The Household Exemption

The household exemption has its origins in the *Directive 95 aimed of balancing right to privacy against right to data protection* that are interrelated, but also different from each other.[59] The GDPR adopted the same approach as the

58 It should have been mentioned in the scenario, that the robot could process such data to detect other diseases than what the user was introduced about, since it would require the data controller to obtain another consent. Another note should have been made about the data that Robinsan processed to reach to the possible drug addiction outcome, based on the following data: processing the data from the eye pupil (size), eye color, face color (yellow color), sudden changes in the emotional status (mimes and voice, words spoken, also facial indications), dry mouth, shaking body or hands, focusing problems, sweat level (without an additional hardware). Possible use of an external hardware such as a chip that could detect the blood pressure, a real time sweat level, identification of unknown chemicals out of the ordinary chemical components, *etc*. could have been inserted in the text.

59 Raphaël Gellert & Serge Gutwirth, 'The Legal Construction of Privacy and Data Protection', *Computer Law & Security Review*, Vol. 29, 2013, p. 524; Juliane Kokott & Christoph Sobotta, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', *International Data Privacy Law*, Vol. 3, Issue 4, 2013, p. 228.

doi: 10.5553/HYIEL/266627012021009001014

Directive 95 and exempted the natural persons executing purely personal and household activities as Article 2 (2/c) of the GDPR states. Recital 18 of the GDPR gives some clues on what purely personal or household activity means, that is, activities performed by natural persons and having no connection to a professional or commercial activity. Activities like this could be keeping a phone book or even using social networking tools. In this case, it would be an easy solution to exempt Julia from the application of the GDPR (as a responsible person), for she was just a simple user. However, *if Julia is somehow identified as a data controller, then it is not possible to apply this exemption* in her case since the controllers that provide the means for processing personal data for such activities are subjected to the GDPR. The means for processing were interpreted in several opinions[60] and guidelines,[61] as it could involve the natural persons as data controllers even if it is of the limited application,[62] like sharing other people's personal data online.[63] In the scenario where Robinsan infringes privacy (for the other people), Julia might be considered as a data controller in a very limited case, but still, she has duties in fulfilling her informing obligations and consent requirements as the interpretation in the *Lindqvist* and *Ryneš* cases show.

The *Lindqvist* case[64] was brought before the CJEU in the years when the Internet became accessible for personal use. Mrs Lindqvist established a webpage for a group of friends who knew each other from a parish. The website was operating offline, meaning that it was accessible only by the ones who had the link. While she was keeping some of her colleague's personal data such as names, some sensitive data was also kept on the website such as a colleagues' health condition. Even though Mrs Lindqvist removed this data from the website upon her colleagues' request, the Swedish NSA referred the case to the CJEU seeking an answer to whether such data processing activity falls under the household exemption. The CJEU took the position that the exemption applies only to those actives, which are carried out in the course of private or family life of individuals, "not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people."[65] Further, while she did not notify her friends about the existence of the website, she missed the opportunity to ask for their consent, therefore she was liable in failing to fulfill her information obligations and to obtain consent of her colleagues. In the scenario, if Robinsan would have disclosed the health condition of Julia's son's to someone else, the household exemption never would have been

60 Opinion of the European Data Protection Supervisor on the Commission's Communication on Unleashing the Potential of Cloud Computing in Europe, European Data Protection Supervisor, 16 November 2012.

61 Statement of the Working Party on Current Discussions Regarding the Data Protection Reform Package-Proposals for Amendments Regarding Exemption for Personal or Household Activities, Article 29 Working Party, 2013, p. 5.

62 *Opinion on the Recent Developments on the Internet of Things 8/2014*, Article 29 Working Party, p. 14.

63 *Opinion on Online Social Networking 5/2009*, Article 29 Working Party, p. 7.

64 Judgment of 6 November 2003, *Case C-101/01, Bodil Lindqvist*, ECLI:EU:C:2003:596.

65 Opinion of Advocate General Tizzano delivered on 19 September 2002, *Case C-101/01, Bodil Lindqvist*, para. 47.

doi: 10.5553/HYIEL/266627012021009001014

a question. However, even in the current situation, there is a risk for data to be obtained by others (indefinite number of people), meaning that household exemption should not be applicable.

One may still think that operating a robot at home for personal purposes does not raise liability issues like obtaining consent and fulfilling information obligations. In the *Ryneš* case[66] Mr Ryneš placed a CCTV camera (closed-circuit system to which only the user had access to the data) that helped to identify the people that repeatedly attacked his home, the Czech NSA claimed that he failed to fulfil his obligations as a data controller. The case was referred to the CJEU, which stated that the camera was used for identifying people whose data was processed in an automated meaning and was meanwhile recording a part of the public space. The CJEU did not treat the question whether Mr Ryneš was a data controller but confirmed that he failed to fulfill his information obligations and the consent obtaining requirements. In the scenario, Julia brought the robot home, which could monitor not only her daily routines but also other people entering her home. Moreover, aside from the Company, she was the one who could deploy and access data in Robinsan, taught the robot how to make use of it for her daily memory activities. Further, she has become in a position that allowed her to aware of her son's drug addiction issue, and she might, have visited a doctor to seek a solution for her son based on her legitimate interest, which raises the risk that the data could be accessed by third parties.

In light of the case-law, it is safe to state that if a data controller collects data from public spaces or if there is a potential for the processed data to be accessed by other people, then the processing activity surely does not fall under the category of personal or household purposes. In order to operate a robot, the data controller(s) must fulfill some obligations, such as providing information, obtaining consent, or giving the possibility to the data subjects to withdraw their consent. The space Robinsan was actually used in, is partially public (people entering home) and people under Robinsan's surveillance should have been informed about its operation. On the other hand, Julia, as the main user, is also under surveillance, so first the Company shall inform both Julia and the people entering home and should obtain their consent. Then, Julia shall fulfill at least her information obligations as a potential data controller. The way a valid consent should be obtained and the type of what information that should be presented (to the actual and potential data subjects) will be discussed under the Consent Question.

5.1.2. The Consent Question

There is no difference between the natural and legal persons in terms of their liabilities in fulfilling the information obligations and obtaining consent based on the GDPR. The data controller, either a natural person or a legal person, are both bound to follow standard rules related to consent. In the scenario, Robinsan's Company is strictly obliged to inform Julia based on the Articles 12, 13 and 22 of the GDPR, as well as to obtain her consent for operating the robot based on

66 Judgment of 11 December 2014, *Case C-212/13, František Ryneš*, ECLI:EU:C:2014:2428.

doi: 10.5553/HYIEL/266627012021009001014

Article 7 of the GDPR. One may discuss whether the consent would be the right legal basis for operating Robinsan, and the legitimate interest legal basis should be brought up instead. Since Robinsan processes sensitive data (*e.g.* health data) and data based on an ADM, which raise a great risk to the rights of the data subjects, and Robinsan is able to process data for a wider scale of purposes than expected, the legitimate interest may not be appropriate in this case. Based on the daily practices, as well as the fact that no other legal bases could be feasible for processing activity to ADM (*e.g.* processing necessary for the performance of a contract or necessary for compliance with a legal obligation, *etc.*), consent would constitute the best choice for the Company.

Obtaining a valid consent (as well as an explicit consent in the case of processing health data) is mostly about the rules and principles related to providing transparent information, purpose limitation, complying with the conditions of consent and information obligations. There are court interpretations on how the validity of consent could be better ensured in conformity with the rules laid down in the GDPR. For instance, in *Planet49*[67] where an online gaming company that placed two pre-ticked consent boxes enabling cookies to collect personal data from the website visitors' devices, one of the questions referred to the CJEU was about what information the service provider has to give within the scope of the provision of clear and comprehensive information to the user in order to be able to fulfill informing obligations. In the analysis of the case, Advocate General (AG) Szpunar[68] pointed out an important aspect of the cookies which refers to the technical complexity refraining the average internet user from fully understanding how they really function. Moreover, the AG stated in his opinion, that if the data controller does not present sufficient information to the data subjects who already rarely checks the content of the pre-ticked boxes offered online, this puts them in an asymmetrical situation (before the provider).[69] However, the user must be able to assess the consequences of the data processing activity and then give consent; therefore, they should be fully informed before giving their consent. The CJEU, in line with the AG's opinion, further emphasized that the consent text should be presented "with sufficient clarity from a typographical point of view"[70] to ensure that the data subject has considered the consent boxes. Still, the interpretation of the case does not clarify the problem of providing understandable information to each data subject, and in personal basis, as discussed before.

The second issue to be discussed here is related to the question of whom the consent shall be given to, if there are more people involved in data processing than a data controller. It is crystal clear that the Company should have obtained Julia's consent, but what about the people entering her home? Even though Julia

67 Judgment of 1 October 2019, *Case C-673/17, Planet49*, ECLI:EU:C:2019:801.

68 Opinion of Advocate General Szpunar delivered on 21 March 2019, *Case C-673/17, Planet49*, para. 114.

69 Id. para 37. *See also* Orla Lynskey, 'Track[ing] Changes: An Examination of EU Regulation of Online Behavioural Advertising Through a Data Protection Lens', *European Law Review*, Vol. 36, Issue 6, 2011, p. 880.

70 *Case C-673/17, Planet49*, para. 35.

doi: 10.5553/HYIEL/266627012021009001014

is not a joint data controller, and her liabilities as a natural person are milder than the Company's, it is arguable to whom the consent should be given regarding the people entering her home. Should the Company receive even more surveillance power and process people's data, or it should be the user who controls the process? In *Wirtschaftsakademie*[71] a university created a Facebook fan page, and the question was whether it would be the Facebook or the university that should have obtained the consent, despite the university was only a user. The interpretation of the CJEU pointed out that, processing could not have occurred without the prior decision of the university to create and operate a fan page on Facebook,[72] therefore it should have been the university obtaining consent (as a joint data controller). In the *Fashion ID* case, where the company, FashionID, embedded a Facebook like button in its website, and so the same question was referred to the Court and had been analyzed. Even though the FashionID claimed that it had no means of controlling the personal data of the website visitors, the CJEU took the position that it facilitated data collection even though it did not have any control over the data.[73] Therefore the consent should first have been obtained by the Fashion ID since the visitors first consulted the website, which triggered the data processing.[74] Turning back to the scenario, Julia could have at least inform the people about the existence of Robinsan, by providing some basic information, such as the data it might collect and for what purposes, whom the data is being disclosed, the duration of storage, and whom to contact in case they wish to exercise their rights, similarly as Mr Ryneš and Mrs Lindqvist should have done. The information that should have been provided to the potential data subjects and the information the Company should have provided to the data subjects remains vague, due to the complexity of assessment of the functioning of robots. Moreover, there has not been a case yet assessing the concept of the information that should be provided to the data subjects in case an ADM deployed in an embodied machine.

5.2. Part II. Expert Opinions

This section will present the expert opinions that are firstly given as a general evaluation of the questions and the scenario, and subsequently an analysis specific to the questions discussed in Part I. Personal opinions of the experts will be presented with the following quotation form: "Expert from (country X)" and a randomly assigned numeric to differentiate. Country names are abbreviated as follows: Finland "F", Hungary "H", Italy "I", and the Netherlands "N".

As a general evaluation, most of the experts (10 experts in total) said that such a technology referred in the scenario either has already been happening or would surely happen within 20 years. All experts unanimously stated that the GDPR is completely applicable to the scenario, however, regarding the application

71 Judgment of 5 June 2018, *Case C-210/16, Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2018:388.

72 Id. para. 56.

73 Judgment of 29 July 2019, *Case C-40/17, Fashion ID*, ECLI:EU:C:2019:629, paras. 74-75.

74 Id. para. 102.

doi: 10.5553/HYIEL/266627012021009001014

of the GDPR, Experts H4, H5, and H6 noted that the problems raised in the scenario are already existing ones. This statement somewhat confirms the previously made analyses. Expert H6 added that the GDPR was introduced into the EU's legislation very late, and still without considering the emerging technologies, so this could raise some difficulties in the application. Expert F1 and N4 noted that besides the GDPR, a *lex specialis* could also be applicable to the questions referred to in the scenario. The Expert F1 pointed out that Robinsan was a medical device and there is already relevant legislation[75] (although they have not yet been harmonized in line with the GDPR). Even though the experts agreed on the complete applicability of the GDPR on the scenario, some of them are unsure about the right implementation, since there are lack of practices and interpretation. After a year of collecting the expert opinions, the EC released a draft regulation on AI[76] including new rules on processing data with AI, confirming these statements.

5.2.1. The Household Exemption and Responsibilities of the User

Even though divergent opinions were given on the applicability of the household exemption, most of the experts (11 experts) stated that *the exemption was not applicable since there was an automatic data processing activity operated by the robot*. Regarding the liability question, there was significant difference between the approaches of the NSA experts and lawyers. Lawyers were quite clear about that the liability should be shared between the Company and Julia, while the NSA experts approached suspiciously to the operability of this action. For example, Expert H4 stated that the Hungarian NSA probably would not accept this claim in the first place. However, some of the experts (8 experts) agreed on Julia's data controllership and the fact that she should have carried out certain liabilities, like fulfilling the informing obligations. This approach was also divergently adopted by the experts, located even in the same country. While Expert N1 was sure about Julia's data controllership based on the fact that she was the one feeding Robinsan with data and teaching the robot how to evaluate it, Expert N3 did not agree with Julia's data controllership and that she should be on the same liability level as the Company. In Italy and Finland, the possibility for a natural person to become a data controller is almost impossible. In the Netherlands, some of the law offices would consider assigning the controllership also to natural persons in addition to the legal persons. In Hungary, there might be even more diversified approaches; experts independently from their affiliations – would interpret the case differently – the Hungarian NSA or among the lawyers, there would be different approaches to the question. As a result, it can be concluded that the scenario and the question on the household exemption raises complicated interpretation on the probable data controllership of the users of certain

75 Council Directive 93/42/EEC of 14 June 1993 concerning medical devices; Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices. These directives are apparently quite old-dated; since 1990 technology in medical sciences has also been drastically change and these Directives' applicability also could be a question for another research.

76 *See* at https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN.

doi: 10.5553/HYIEL/266627012021009001014

emerging technologies and these cases would probably have divergent interpretations at the national courts. It was certain that the data controllers must have fulfilled their information and consent obligations, and the experts were further addressed the question of how these obligations should have been fulfilled.

5.2.2. Consent and Informing Obligations

The available literature, as well as the analysis conducted in the Part I, showed that *ensuring the validity of the consent of an HSR user is very difficult, if not impossible*. Almost all the interviewed experts shared the same view that the purpose limitation and transparency of algorithms in robotic brains are among the most difficult issues to ensure from the data protection point of view. They also think that consent alone would not be enough for comprehensive data processing activities, but the other legal bases, such as performance of a contract or legitimate interest rules would constrain the data controller's business logic. Therefore the data controllers would still hold the tendency to use consent as a legal basis, just as it was stated in Part I.

Experts indicated different aspects on the difficulties in obtaining a valid consent, as well as providing concrete information about the purposes on data processing in robotics. Expert I1 stated that the Robinsan's system should have been constrained in a way that only the expected purposes would have been fulfilled, but the Expert would also welcome to receive personal suggestions by Robinsan to make life easier (*e.g.* the robot could 'guess' the users eating habits from the goods in the fridge and suggest some restaurants accordingly). While these suggestions fall far from the exact purposes, the Expert agreed with the fact that putting an exact border on the processing purposes is a difficult task, confirming the impossibility of limiting the purposes. Expert F1 evaluated the consent in the scenario as similar to the practice (where data subjects about all the possible data processing activities as well as the risks arising from processing) of the American companies, and which is not acceptable in Europe. Expert F2 noted that obtaining consent is the pure duty of the company, but the way the company should do this is a difficult question, since using such a robot may have multi-way effects in the real life. The Expert thinks that the user's condition could be a starting point in generating user-specific information, meaning that the information to be provided should be personal, and not generic. The Expert believes that ensuring valid consent is a fiction and the data controllers in Finland are not aware of how invalidly they obtain consent.

The experts also stated that it is hard to clearly identify how the robot user and the company should obtain the data subjects' consent. Expert N1 expressed that while obtaining Julia's consent while being a data subject was purely the liability of the Company, Julia also should have informed the people entering her home about Robinsan. in order to do that, she must have been informed every aspect of Robinsan by the Company, from the operational aspects to the risks. Expert H5 strongly believes that Julia must have obtained other people's consent when they entered her home without an exception, otherwise she should have switched the robot off. Finally, Experts F1, N1, and N3 remarked that there is no

doi: 10.5553/HYIEL/266627012021009001014

rule for ensuring the understandability of the information in the GDPR that data controllers provide to the data subjects. Similar to the analysis made before, the experts referred to the GDPR's general rule on understandability of the information by the average data subjects trespassing the importance of designing a personally tailored information. When patients or elders are the robot users, their health conditions (Expert F2), cultural identity, age, education, (Expert I2), and their vulnerability (Expert H1) must be taken into account when providing information. However, such rule is not directly inserted in the GDPR, and some of the experts share the position that it could be found in the consumer protection law, instead the GDPR.

Finally, the experts were asked to deliver their opinions on the humanoid outlook and behavior of social robots and their influence on data subjects to freely give their consent. All the experts stated that the GDPR cannot prevent data controllers from designing such systems that are encouraging people to disclose more data. Some of the experts (Experts H2, N3, and F2) said that the GDPR should not restrict companies in this sense. Expert H1 added that it might be even a positive aspect if a robot encourages people to include them in their lives since there are many lonely and desperate people in Europe, but they must also be aware of the consequences of their interaction with the robot. Expert H4 does not think that this is related to the GDPR, but to consumer protection (shared view by the Expert N6), in a way that persuasive robots might breach consumer rights. Expert N6 thinks that this question is related to ethics, in addition to consumer protection, and stated that it is a very interesting question to be given further thought. *Uncanny Valley is true, but there is no uniform legal rule preventing it to happen in real life*, if not complicating the essence of the questions raised in this work.

6. Conclusion and Recommendations

This work presented a case-law analysis supported by scenario and interview methods that were used to test hypotheses deriving from comprehensive literature analysis on the applicability of the GDPR on HSR. As a result of the analyses, several practical problems were identified regarding to the consent rule; data subjects do not fully understand the privacy statements and they are not always conscious about the possible consequences of AI technologies, especially HSR. They might share other people's data with robots or could disclose other people's data without being aware of their liability obligations Data controllers operating HSR might not always be able or might not wish to present fully understandable information to their users on the use and risks of HSR.

Technical aspects of AI technologies make it hard for the data controllers to completely comply with the GDPR. Their unpredictable data collection and processing by design may not always make it possible to put very clear statements on purposes the HSR is operating for. However, this should not mean that the data controllers could be exempted from their obligations and responsibilities. Algorithms might generate unpredictable outcomes, but as long as they fall

doi: 10.5553/HYIEL/266627012021009001014

outside of the purpose of the AI system, data controllers must ignore them and not display those purposes to the service of the users. The GDPR cannot prevent robotic companies to produce such robots gaining the trust of people and make them disclose more personal issues. The companies even should not be restrained from doing so since trust may increase the level of the user's treatment. Eligible safeguards specific to this technology should be introduced in the application.

As a result of the analysis above, it can be concluded that complicated cases will be emerging with HSR and their data processing activities within the purpose of serving their users. In order to avoid such these problems, several steps could be taken by the actors involved by either creating or interacting with the robots and further suggestions could be taken into account.

6.1. For Data Controllers

This work proposes a compulsory user education and training program to be prepared by the data controllers about the system usage such as including training for the system's technologic elements, providing tools for personal data management, raising the user's understanding on the possible risks on their right to personal data protection. Further, the trainings should contain several user cases through scenarios and should be shared with the users based on their person-specific case. Data controllers should engage users in the development and testing phase of the robot, or during the course of conducting the DPIA as suggested by Article 29 WP's DPIA opinion in line with Article 35(9) of the GDPR.[77] Pieces of training must be set by the level of user's understanding and this understanding must be verified and proved. Obligatory lifelong training programs should be offered for the people using AI systems so they would be able to catch any new developments within the system and to ensure the full compliance during the lifecycle of the systems. Data controllers should provide these programs by organizing some informative presentations for the other possible data subjects, mainly to the family members of the main user. All training shall be provided free of charge. Trainings should be personalized and the implementing of specific ML techniques for creating user-specific training content could be time and cost-efficient.[78] This way, full user control on the AI system could be ensured. An additional comprehensive internal training program for the company staff could help to raise the awareness of its own staff.

77 Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/67, Article 29 Working Party, p. 15, and Article 35(9) GDPR links seeking the data subjects 'views in a "where appropriate" clause, so explaining the cases where it would be appropriate to include the user views in the DPIA could be a good start. Otherwise, introducing a new legal requirement pointing the user views and experiences in a new legislation would be a better idea.

78 For example, the robot could act as an agent to analyze the user's personal informational choices and bring only that information to be read and understand by the user. Even more, the robot could be the cyber representation of the user, acting like the user and represent the user's behavior whenever the user should be informed or request information about the system. *See* Marco Conti & Andrea Passarella, 'The Internet of People: A Human and Data-Centric Paradigm for the Next Generation Internet', *Computer Communications*, Vol. 131, 2018.

doi: 10.5553/HYIEL/266627012021009001014

The second solution to be thought of is to ensure that the information which data controllers deliver to the users is valid and comprehensive. If the information prepared for the users should be specific to their personal conditions (age, gender, education, *etc*.) and personality (mood, behaviors, character, *etc*.), they could use or develop AI-based systems analyzing users' privacy needs and design their systems according to the outcomes reached by these analyses. They could further enhance their legal and ethical compilation with developing and using a personalized AI tool detecting the person-specific information needs. They could also bear in mind the AI tools open for improvement aiming to analyze specific groups of people's data to generate its reasoning itself. When an output is reached by a robot and the data subject wants to find out how that output was reached, real-time explanations with the help of computational models (mainly, RL technique) should permit the data subjects to personalize the explanations could be also useful.[79] Robinsan could be deployed with such an assistant answering the questions in this way, for example, to the question of why did you include the leaflet about drug addiction? Then the answer would be,

> "had the subject sweated less than X ml per day and the blood pressure would be around 120/70, the body would not show sudden trembles, also eye bulb would be around normal size, the subject would not be suggested to solve his drug addiction problem."

Besides, data controllers could use very simple, but effective ways to test their users' knowledge of the systems they offer. For example, after the information phase, a small quiz could pop-up on the user's screen to test the level of understanding of the user. This quiz could include basic questions generated from the given information and there should be no way to skip the test if the user wants to continue using the system. In the same way, there could be set up a certain amount of time for anyone to read the consent statements. If someone skips to check the consent box in, for example, in 5 seconds, this should mean that the user did not read it and would fail to continue with the process. They could also place a button on their websites/services interface, such as the robot's image or use a verbal indication, about preventing data controllers to trade or share their data with third parties. A similar solution is already available in the California Consumer Privacy Act.[80]

6.2. For Users/Data Subjects

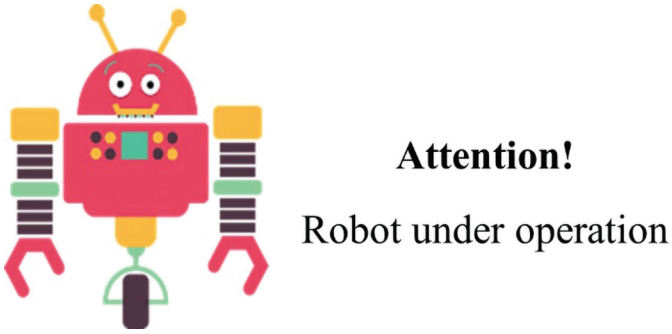
The data subjects acting as users of such technologies should be aware of the dark side of the technologies they use and should bear the fact in mind that they have certain liabilities when using these technologies. Regarding the fulfillment of the

79 In their work, Ehsan *et al*. developed an automated rationale generation for providing such explanations based on real human explanations used for training a model. *See* Upol Ehsan *et al*., 'Automated Rationale Generation: A Technique for Explainable AI and Its Effects on Human Perceptions', *Proceedings of the 24th International Conference on Intelligent User Interfaces*, 2019.

80 CCPA § 1798.135 (1).

doi: 10.5553/HYIEL/266627012021009001014

Figure 1 ***Example warning sign to be placed in the entrance and inside the home.***



consent issue and information obligations, they could place a sign as it is shown in Figure 1. at the entrance and inside their homes warning the visitors of the operation of an HSR. If someone does not wish to be under the surveillance of the robot, the user shall shut it down and shall not put stress on family members and visitors to accept the robot against their will. The sign should be provided by the data controller after the compulsory trainings and should be one of the prerequisites of obtaining the GDPR compliance certificate (mentioned below) for the data controllers.

6.3. For Lawmakers and for the Data Protection Authorities

Bearing in mind the speed of the technological developments and the variety of the available tools, lawmakers could gain from scenarios to better design future-friendly law to avoid unwanted ethical and legal consequences. For the NSAs, some operable solutions could be discussed, ideas coming out from the already existed legislation. The first suggestion is related to operating Article 42 of the GDPR, which calls data controllers to voluntarily have certificates proving their GDPR compliances. The certification includes not only paperwork but also seals and marks for their products and services. It would be a good idea to introduce a compulsory certification system for the companies offering services through personal house robots, unlikely the voluntary certification system as included in the GDPR. *The certification could be established under at least three criteria. (i)* Compulsory user education and training, as mentioned before, to place under the oversight of the NSA in collaboration with the specific national authorities related to the service offered (*e.g.* National Alzheimer Association). *(ii)* Compulsory user and company licenses: without the user license, the user cannot purchase the robot; and without the company license, the company cannot produce the robots. The idea is as simple as it is in the case of driving licenses; people who do not have a driving license cannot drive a car legally. Applying this idea to the personal household robots, users should be designated a specific license to have a personal robot at home. User licenses should be valid for maximum a year and the user must meet certain criteria to renew the license (*e.g.* accomplishment of a new training offered by the company). Such a solution

doi: 10.5553/HYIEL/266627012021009001014

already exists for developers choosing a safeguard plan for themselves against the possible misuse of AI solutions by any user.[81] As for the company licenses, they should be first obtained from the competent authority (*e.g.* EU Agency for Robotics and Artificial Intelligence), from a national institution or from a new authority to be set up (*e.g.* Hungarian Ethics Center[82]). Data controllers that obtained the license could place a seal on their products or services indicating their GDPR compliance. *(iii)* Compulsory insurance system: when the creators and users are found jointly liable or when the liable person cannot be identified because of the robot's autonomous actions, the insurance system should cover the costs of the damaged parties.

Finally, it would be practically useful if the NSAs could broaden their knowledge of emerging technologies and generate more guidelines for the better implementation of the GDPR in this sense. For example, the ICO, in cooperation with the Alan Turing Institute, already published a guideline explaining the decisions made with AI.[83] The NSAs could either benefit from the other NSA's experiences and knowledge, or create their own collaborative works specific to the questions raised in the country in which they operate. Organizing events or being involved in projects focusing on AI and the GDPR surely would guide the NSAs on how to start and provide the necessary technical information that would, in the end, guide the data controllers to understand and implement the GDPR better.

81 *See* at www.licenses.ai.

82 *Hungary's Artificial Intelligence Strategy 2020-2030*, Ministry for Innovation and Technology, May 2020, p. 34.

83 ICO 'Explaining decisions made with AI', 2020.

doi: 10.5553/HYIEL/266627012021009001014