Application of the General Data Protection Regulation on Household Social Robots

Doctoral (Ph.D.) Dissertation

Gizem Gültekin dr.Várkonyi

Supervisors:
Prof. Dr. László Trócsányi
Szilvia Dr. Váradi Dr. Kertészné

University of Szeged
Doctoral School of Law

Szeged
2020

Abbreviations

ADM	Algorithmic Decision Making
AG	Advocate General
AI	Artificial Intelligence
CEE	Central and Eastern European
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPA/NSA	Data Protection Authority or National Supervisory Authority
DPbD	Data Protection by Design
DPIA	Data Protection Impact Assessment
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EP	European Parliament
EU	European Union
GDPR	General Data Protection Regulation
UDHR	Universal Declaration of Human Rights
OECD	Organization for Economic Cooperation and Development
WP29	Article 29 Working Party
HSR	Household Social Robot
HRI	Human-Robot Interaction
IoT	Internet of Things
ML	Machine Learning
MS	Member State
RRI	Robot-Robot Interaction

Figures and Tables

Appendix

Acknowledgments

“All the praises be to Allah, Lord of the worlds –
The Most Gracious, the Most Merciful”
Al-Fatihah 1:1-2

I think a doctoral dissertation is never a single person’s production. I would like to mention here everyone contributed in the successful accomplishment of this dissertation.

First of all, I would like to thank my Turkish family for their complimentary support for all my life and for in any case. I know that we are far in distance, but we are one in spirit. Bu hayatta başardıklarımı bana verdiğiniz karşılıksız destek ve sevgi sayesinde, birbirimizden uzakta olsak bile kalplerimizin hep bir olduğunu bilerek başardım, canım ailem.

I would like to thank my Hungarian family for the same complimentary support. It would be impossible to build my life and my career in such a good way without a single support, patience, and understanding of my husband. Szeretném megköszönni a támogatást a magyar családomnak is. Lehetetlen lett volna ilyen jó módon felépíteni az életemet és a karrieremet, férjem támogatása, türelme és megértése nékül.

I acknowledge Prof. Dr. László Trócsányi and Dr. Márton Sulyok as part of my family. Thank you Professor, for being such a great supervisor, sharing all your academic and professional knowledge with me, for providing me a place and a network to improve myself, and for truly taking care of me. Thank you Márton, for your trust on me, for all the opportunities you created for me and for helping me to improve my academic and professional life in this way. There is more to thank both of you, but the space in here is not enough for all.

I am proud to be a part of my Turkey and my Hungary. I would like to dedicate this work to the Crescent Star, as well as to the Holy Crown.

It would be impossible to start, develop and complete this work without a single help of my supervisor, Dr. Szilvia Váradi-Dr. Kertészné. Thank you for sharing your rich knowledge with me generously, for your time, and the guidance you provided for me. Many thanks also to Dr. Attila Kertész for his entire help.

I further would like to thank to Dr. Anikó Szalai and to Dr. Zsuzsanna Fejes for their entire help and support during my journey. I am also indebted to my colleague, Tünde Silay, thank you.

I wish to extend my deepest thanks to the University of Szeged, Faculty of Law, International and Regional Studies Institute, Doctoral School of Law, Tempus Public Foundation, Hungarian Ministry of Justice, Turkish Ministry of National Education, and Hungarian Data Protection Authority, for the resources and the opportunities.

Many people helped me to improve and accomplish this work (hereafter the names are listed in an alphabetical order). Many thanks to Anton Gradišek, Akif Berber, Bedrettin Gürcan, Prof. Gordon Hunter, Martijn van Otterlo, and Zsuzsanna Mátrai for their contributions to develop the ideas in the scenario. I gratefully acknowledge the help I received from Dr. Endre Győző Szabó, Prof. Dr. Jaap de Zwaan, Prof. Dr. Oswald Jansen, and Prof. Dr. Maurizio Mensi for their time and effort in connecting me with the great experts to make the

interview happen. It would be impossible to complete this work without the experts who kindly shared their time and knowledge with me, thank you: Aarnio Reijo, Ádám Liber, Chris Koppe, Federico Marini Balestra, Jukka Lang, Marlies van Eck, Dr. Márton Domokos, Max Rozendaal, Sandra van Heukelom-Verhage, Paul Severens, Dr.Tamás Bendik, Dr.Tamás Bereczki, and Dr.Tamás Parti.

I am very thankful to Dr. Dániel Eszteri and Dr. Róbert Szuchy for generously sharing their knowledge and opinions with me to make this dissertacion work ready.

Finally, I would like to thank to the team of the Interdisciplinary Summerschool on Privacy'18 and of the Academy of European Public Law'18-'19 for the academic, scientific and networking opportunities.

Here, standing at the end point of this long journey, I acknowledge that what I spent for creating this work totally worth, and even though one believe that could do always better, I am fully satisfied with this work.

I. Introduction

Artificial Intelligence is probably one of the most popular topics of the last five years and it was mentioned more or less almost in any field. AI and robots today appear in healthcare, transportation (including interspace transportation), construction, goods and services delivery, financial services, education[1], in short, in every field of life. Indeed, there is a sound reason for that. AI-enabled health care technologies could predict in the treatment of diseases 75% better than the traditional tools and could reduce the clinical errors 2/3 at the clinics using AI compared to the clinics do not[2]. AI-enabled technologies could handle repetitive jobs, therefore could help saving time and cost for businesses, for employers, and employees. Industrial robots could execute such tasks in a way with less or no risk, otherwise to be dangerous and risky for humans (e.g., landing on Mars or mine exploding). Many more benefits could be further listed, however, the point where the attention should be drawn is that the era of human-robot collaboration has started. This era will be engaging people to interact, cooperate, and benefit from the AI and robotics technologies thanks to the easily accessible and available Big Data, besides the developments and decreasing costs of hardware, and increasing engineering skills. Such opportunities encourage the public and private sector to keep investing in, therefore the AI investment explosion promises this technology to be soon as part of people's life.

The AI market currently worth around USD 664 million and is expected to grow to USD 38.8 billion by 2025 according to the EU[3], and is expected to grow 190.6 billion by 2025, according to another forecast[4]. Either the actors in businesses and industry or the governments invest in AI technologies, maybe different in volumes, but the governments promise the investment in their annual budgets by completing it in their National AI

[1] "Sizing the prize: What's the real value of AI for your business and how can you capitalise?", [Online], PwC Global, Accessed from: https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html Last accessed: 19 January 2020

[2] "The AI effect: How artificial intelligence is making health care more human", [Online], study conducted by MIT Technology Review Insights and GE Healthcare, 2019. Accessed from: https://www.technologyreview.com/hub/ai-effect/ Last accessed: 20 January 2020.

[3] Opinion of the European Economic and Social Committee on 'Artificial intelligence -The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society' (2017/C 288/01)

[4] "Artificial Intelligence Market by Offering (Hardware, Software, Services), Technology (Machine Learning, Natural Language Processing, Context-Aware Computing, Computer Vision), End-User Industry, and Geography- Global Forecast to 2025", [Online], Markets and Markets.
Accessed from: https://www.marketsandmarkets.com/PressReleases/artificial-intelligence.asp Last accessed: 20 January 2020

Strategies[5]. Big-tech companies, such as Facebook, Google, Apple, Alibaba, etc., have been announcing new AI projects specifically designated for AI and robotics research at their research departments. The EC is to launch a new long term funding for 2021-2027 with a 9.2 billion Euro budget to support the so-called Digital Single Market that involves AI research and development activities[6]. While the investments raise in sectors, the topic raises popularity in academia and the public. AI and particularly Human-Robot Interaction presented by service robots have been increasingly reported by the news magazines since the beginning of the 2000s[7]. Academia also pays significant attention to the topic. Several scientific papers entitled with ML researches have grown twenty times, while the robotics topic grew thirty times in 2019, both compared to 2010, in the arXiv pre-print repository[8]. Only in 2019, we participated in several scientific events organized around a topic that is not mainly focusing on AI, but also hosted AI discussions during the events. AI, without a doubt, will continue to be a topic of a discussion in any field, let it be science and technology, legal, economy, medical researches, or ethics.

During the preparation phase of this work, different approaches focusing on the distinction between, as well as the uniformness of the terms AI and robots were detected. The present dissertation will not differ AI and robots, the readers of this work shall read the terms AI and robots interchangeably. Robotics could be a stand-alone technology without AI but currently, they are deeply engaged and almost meaning the same in the eye of technology, as Figure 1. also shows. The reason why this integration might be that AI can perform more useful tasks in embodied than it could as a software[9]. By being in the real world, AI would be more intelligent and would be perceived as more real[10] that is an important factor in acceptance by a human (also causes deception by humans, will be discussed later). Academia does not separate the AI in form of robots used in practice; for example, Edwards[11] et. al. do not differ a social robot and AI once used for education, by highlighting the communication aspect of a social robot as a teacher as it is simulating a real human to human interaction. Legal academia especially does not differ the AI and robots, for example, Prof. Ryan Calo,

[5] Currently, there are 33 countries have adopted a national AI strategy. Source: Future of Life, National and International AI Strategies. Accessed from: https://futureoflife.org/national-international-ai-strategies/?cn-reloaded=1 Last accessed: 28 January 2020.

[6] Szczepański, 2019, p. 8

[7] Mejía and Kajikawa, 2019, p. 122.

[8] Perrault, et. al., 2019, p. 21.

[9] Nath and Vineet, 2017, n.p.

[10] Leroux et al., 2018, p. 60.

[11] Edwards, et. al., 2018, p.475.

a leading robolaw scholar, identifies robots as embodied AI[12]. From those, personal robots have a special place in academia in which is referred to without a distinction between the two terms. To illustrate, Broman and Finckenberg-Broman's work highlights the HRI as the meeting point of AI and robots and strongly suggests that they should be evaluated together from the legal point of view since[13]. Furthermore, some of the important global actors do not attempt to evaluate AI and robots separately in their official documents. The United Nations approaches the robots from their autonomous feature where AI "enables them to perform complex tasks in changing environment without being teleoperated or controlled by a human operator"[14]. Some of the papers assisting the EU institutions for policymaking approach the robots as "electronic persons"[15], because of their intellectual capabilities and classifies AI as a software acting in the virtual world and as hardware embedded in advanced robots[16].

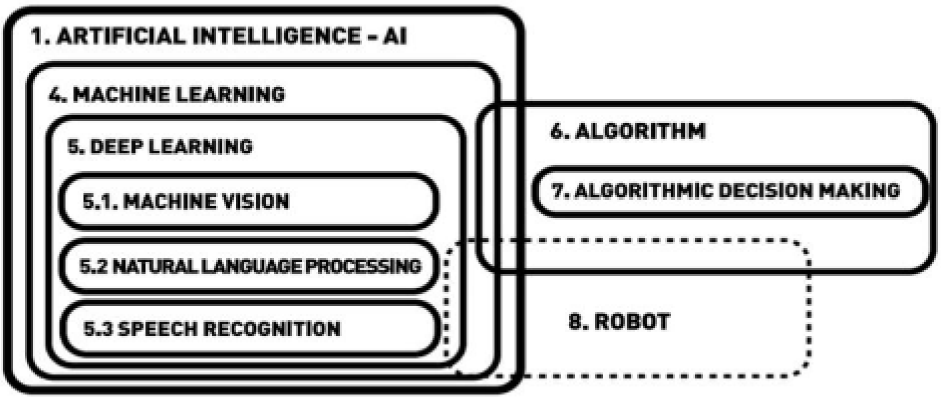


Figure 1. Relationship between Artificial Intelligence and Robotics.
Source: Access Now, 2018, p. 10.

[12] Calo, 2015, p. 532.

[13] Broman, Finckenberg-Broman, 2017, p. 5.

[14] United Nations Report of COMEST on Robotics Ethics, 2017, p. 4.

[15] European Parliament's Legal Affairs Committee, 2017, European civil law rules in robotics. (2015/2103(INL)), para. 59f. The electronic personality concept was one of the novelist solutions offered by the expert by that time but it was quickly put into the shelves by the EC. Later, Bertolini (2020, p.35) developed the idea behind the electronic personality (or electronic personhood with his words) by not thinking this concept as assigning some rights to robots, but creating a quasi-person which the victims could turn to this fictional entity (of robot's therefore the legal persons') to claim their rights from. Indeed, the legal persons behind a robot could be many in terms of number and solving the relationship among each other might be time and even money consuming (see, "Other controllers and processors in the scenario" section of this work). This fictional entity could help speeding up the procedural aspect in case of damage, let it be through insurance or something else, and could ensure the right distribution of responsibilities as well as increasing transparency. Although Bertolini offers this solution in scope of the Product Liability Directive which does not cover software based products or services, it still could be a starting point for more enhanced solutions.

[16] EC, 2018a, p. 12.

By keeping in mind the fact that a simple coffee machine completing repetitive tasks and presenting illusionary intelligence could not be (and should not be) a topic of a high level of analysis, all these indicators were particularly effective using these terms interchangeably the term in a frame of the present work. So, what kind of robot will further be subjected to this dissertation?

There are several types of robots classified mainly under two main categories: industry and service robots[17]. This work focuses on service robots in general, but social robots specifically will be a case for the analysis. Type of robot is an important factor and should be indicated from the beginning, because the risks that will be comprehensively presented in the upcoming sections could easily differ from one type to another[18]. If the present work was done some years ago, it would be difficult to claim a certain future existence of social robots at homes and to talk about the risks they may raise. The reason for this statement would be based on poor tendencies observed in the industry developing AI and robots for personal use back then. Famous humanoid and anthropomorphic robots of Boston Dynamics are developed and tested for military purposes, rather than personal ones. Self-driving cars and drones were those robots one may have heard the most in the news about, not the personal household robots. However, today, personal household social robots are increasingly catching the attention of the industry. For example, the Everyday Robot Project running by the X Development (a subsidiary of Google) aims to create robots to serve in everyday life of humans in "whatever they needed, doing tasks haven't even dreamed up yet."[19] The robot in this project is being developed with ML which will integrate the data that the robot collects through its cameras and sensors at the households. The project's outcome is to make robots possible to work in unstructured environments in collaboration with humans and other robots, especially at households. Facebook, not surprisingly, has been testing the LoCoBot[20] robot, an open-source low-cost robot that could navigate in physical spaces supported with AI navigating without needing a map[21]. Although the full appearance of social robots at

[17] IIFR *Executive Summary World Robotics 2017 Industrial Robots*
Accessed from: https://ifr.org/downloads/press/Executive_Summary_WR_2017_Industrial_Robots.pdf
Last accessed: 8 November 2019.

[18] Fosch-Villaronga, 2018, p. 95.

[19] X Company official website. Available at: https://x.company/projects/everyday-robots Last accessed: 15 January 2020.

[20] LoCoBot official website. Available at: http://www.locobot.org Last accessed: 15 January 2020.

[21] "Facebook has trained an AI to navigate without needing a map.", [Online], MIT Technology Review. Accessed from: https://www.technologyreview.com/f/615078/facebook-has-trained-an-ai-to-navigate-without-needing-a-map/?utm_source=newsletters&utm_medium=email&utm_campaign=the_download.unpaid.engagement
Last accessed: 23 January 2020

households is not yet a phenomenon, they appear at households as cleaning robots such as vacuum cleaner, or as entertainment robots, such as toys, education, and research[22]. Such household robots are about 16 million available in the market and this number is expected to grow to 61.1 million units by 2022[23]. The tendency followed in producing personal household robots shows that people will meet these robots sooner or later in their very private spheres.

On the other side, the engagement of robots in different aspects of human life raises some considerations and risks, as every technology does so, besides their absolute usefulness. People may have to pay the price of a robot by providing their data to the free app deployed in robots without realizing a single risk of doing so[24] such as opening up their private life to a robot. Citizens might be under surveillance by robots appearing in public spaces. Patients may be under stress when they give consent to a robot for their data to be processed, in turn, to receive treatment. Individuals sharing their home life with a social robot may remain unclear liability issues that might be assigned to them. All these risks as well as the benefits are based on the AI systems' ability to process data, especially, personal data in a broad sense.

For these reasons, legal academia and law-makers have been particularly working on discovering the potential risks behind AI technologies. Stressing the challenges and addressing them with a comprehensive approach to reach appropriate policy tools is one of the recent topics discussed under the roof of the EU institutions[25]. Council of the European Union especially calls the related institutions, as well as the MS, to understand these challenges. It draws attention to identifying the specific safeguards related to the use of AI tools. Such safeguards, with the Council's words, could highlight the ethical, social, and legal aspects and needs of the topic, and could even raise new applicable rules to avoid legal uncertainty[26]. This dissertation aims to contribute to the works of the EU policymakers, either to the identification of different problems as of our point of view or offering some solutions that could easily be integrated with data protection legislation (or in a broader AI legislation).

[22] IFR Executive Summary World Robotics 2019: Service Robots. [Online], Accessed from: https://ifr.org/downloads/press2018/Executive_Summary_WR_Service_Robots_2019.pdf Last accessed: 28 January 2020.

[23] Ibid., p. 3.

[24] Free apps and services that those companies offer, not surprisingly, collect more personal data than the paid apps. AGCOM, 2017, p. 27.

[25] Council of the EU, 2020, para. 14.

[26] Ibid., para 20.

AI and robotics is an interdisciplinary topic by its nature giving as a reason that it involves people's individual and professional life significantly and from the different aspects. Scientists benefit from neural sciences, psychology, behavioral sciences and many other different scientific fields when developing social robots. For this reason, and as many of the AI researches do, it would be a wise choice to evaluate the topic with an interdisciplinary approach on a very specific topic. This work adopts a socio-legal approach with a practical point of view, meaning that it will be evaluating purely the applicability of a particular legislation, that is the GDPR, on a particular technology, that is the personal social robots. Readers of this work should not expect a content related to a dogmatic-legal analysis. Keeping in mind the risks that may occur with such an approach, e.g. making an inaccurate calculation or making a mistake, we believe that unless the robots are fully alive and real, there will not be any work that can calculate every aspect of this new technology, not just in a legal sense, but also in the social, economic, scientific and legal point of views. Therefore, being inaccurate or making a mistake is a part of this dissertation where the strong assumptions gathered from the literature form the basis.

Since the present work focuses on the problems regarding social robots and EU data protection legislation, we briefly shall next present the EU's current efforts on the topic which speeded up in the last couple of months before this work was completed.

1. The EU's Current Standing in Regulation of AI

Data protection is one of the concerned areas reflected in the studies conducted by or under auspices of the EP and the EP since the AI technologies could lead the collection and processing of personal data autonomously and unpredictably. AI technologies further enable robots to interact with their environment and gather new data under the supervision of its user through different ML techniques to customize its services in line with the user's needs. While autonomous learning and autonomous decision-making maximize the robots' operability, questions related to designing data protection-friendly robots protecting both its users and the other people around privacy who interact with robots have also started to be a part of these studies.

The EU has been putting a significant effort into the discussion related to the regulation of AI and robotics technologies at a strategical, ethical, and legal point of view. Data protection and privacy is the very first area in which the EP and the EC are being called to review the current legal implications. The very first attempts towards the identification of the problems related to the regulation of AI and robotics technologies in the EU were initiated by several working groups formed under the EP. Among those, the work concluded in 2015 by the Committee on Legal Affairs discussing the civil liability of robotics is one of the first and attention-grabbing ones, kicking off the preparations towards the regulation of AI in the EU. The document turned out a motion for a resolution in 2017 addressing the three important aspects to pay attention in AI regulation: robot surveillance, unclear liability distribution, and ineffective consent implementations appearing during the use of robots. Following this kick-off, the EP's interest in the topic has continuously been increasing up to date, consisting of most of the EU-AI literature including few in quantity but significant policy papers generated by the EP and the EC.

1.1 The European Parliament Working Papers

A report prepared in 2016 by the EP Science and Technology Options Assessment-STOA group[27] enlarged the content of the previous work and start discussing the data protection issues more deeply by identifying seven legal areas that robotics technologies (which they call as Cyber-physical systems) would make it necessary to review: Transportation, trade, civil liberties, safety, health, energy and environment, and horizontal issues. While concerns related to data processing were addressed almost in all these areas, the civil liberties area was dedicated only to data protection. A remarkable observation in this document should the fact that the very first concern referred was related to home-care robots, such as healthcare robots, that could collect and process personal data. Furthermore, algorithmic transparency, risks arising from using a robot for household activities, data ownership, and data share, as well as the relationship between data controllers and data processors were some of the issues identified as challenges. The report was finalized with a recommendation which is about safeguarding these issues pro-actively and in a human-centric way with the help of law, and especially, with data protection legislation. The EU data protection community reacted to this call and dedicated the 38th International Conference of Data Protection and Privacy Commissioners meeting held in 2016 on AI and privacy challenges[28]. This meeting raised specific attention to the transparency and explicability issues in AI systems. The meeting report placed important questions in this sense, such as asking "Who is the data controller for an autonomous machine with self-learning capabilities?". Such a question indeed points to the risks that may be faced in practical AI applications. While the topic was discussed

[27] EP, 2016, p. 7-10.

[28] EDPS, 2016, p. 9.

superficially in those days, upcoming works of the EU became evidential on the EU's wish to take some more tangible steps to understand the topic and raise some solutions.

In 2019, the EP paid significant and increased amount of attention to understand the topic and several EP Committees requested reports and briefings from a variety of experts, therefore. These reports are important to see at what stage the EP is thinking about the regulative issues since there has not a significant policy step that has been taken. Among those, a report requested by the EP's Committee on Industry, Research and Energy summarized that privacy is one of the obstacles setting the EU back from having a strong place in the world, giving as a reason that strong privacy rules push back big companies to invest in EU on AI development projects.[29] In the comprehensive European industrial policy on artificial intelligence and robotics reports, the EP calls the EC to take necessary legislative steps, either is a revision or lawmaking, to solve this problem[30]. Moreover, the EP points a specific topic to pay attention as such is the necessity to ensure "unambiguous and informed consent " and the responsibility of AI developers to develop and follow procedures for valid consent"[31]. Elaborating the topic from the consumers' point of view, the report repeats data protection as one of the areas of concern, since principles such as purpose limitation and data minimization are not the rules easy to comply in the AI age.[32] In this case, the report points that there is a need for building trust towards AI technologies, both from the investors' and the consumers' point of view (and the citizens' point of view, naturally), and adopting more clear and applicable data protection rules seem to be a starting point.

Besides the regulation of AI technologies in general, the EP gave a specific place for understanding the regulation of robotics, too. To identify issues specific to the regulation of robotics, some of the subject-specific events were held at the EP. For example, "Robots in Healthcare: a solution or a problem?" workshop was held in February 2019 under the auspices of the EP to provide information and advice for members of the Environment, Public Health and Food Safety Committee about the robots in healthcare. The workshop report refers to the challenges in the EU health care sector per increasing needs of people to health care services and identifies health care robots as a solution[33]. Especially, care and socially assistive robots were mentioned as some of the most interesting applications in

[29] Delponte, L., 2019, p. 16.
[30] EP, 2018, para. 110.
[31] Ibid., para. 129.
[32] Sartor, 2019, pp. 4-5.
[33] Dolic, Castro, Moarcas, 2019, p. 8.

health care[34]. Report hosts the minutes of the presentations given in the workshop, each pointing data protection, and privacy issues one of the obstacles before these technologies[35]. Obviously, personal health care robots which may also have social interaction capabilities raise concerns towards the right to data protection.

For the present work, the most remarkable report was prepared upon the request of the EP's Committee on the Internal Market and Consumer Protection evaluating the social robots specifically[36]. The report refers to chatbots and social robots as examples of successful AI subfields since they engage people with more interaction, on the other hand, causing more data disclosures by the data subjects. Surely, this report also refers to privacy and data protection issues as a risk category. This report encouraged the EP to draft a resolution currently published and calling the HLEG to review the GDPR, besides other legislation, whether it could respond to issues arising from AI and ADM, and that it could ensure a high level of consumer protection[37].

This call was heard by the EP's STOA and the first study assessing only the personal data and AI relationship, together with its risks and opportunities and policy recommendations, was released in June 2020 prepared by Sartor[38]. His study entitled "Impact of the GDPR on artificial intelligence" gave a specific overview of the risks arising from the evaluation of personal data in AI systems. These risks are, in addition to the others mentioned before, investigated in detail and reported only when it is connected with the GDPR. The risks arising from the possibility of re-identification of the person whose data was subjected to the training data, and of excluding the outcomes of the algorithmic evaluation from the GDPR[39] are remarkable in this sense. Comprehensive profiling leading extraction of new personal data and data repurposing[40] consists of another risk group specific to AI and the GDPR. The study analyzes how AI may challenge the rights of data subjects granted in the GDPR and notes that the data subjects may not easily exercise their right to access, right to erasure, right to portability, and right to object. Personal data definition, consent, profiling, transparency, and purpose limitation are the common topics subjected to both the present work and Sartor's work. Sartor also discusses data minimization, accuracy, and storage limitation rules of the

[34] Ibid. p.7
[35] For example, Dr. Kathrin Cresswell noted four barriers decreasing the number of benefits of health care robots and one of them, not surprisingly, is the ethical and legal challenges. Ibid., p.12.
[36] Przegalinska, 2019, pp. 4-6.
[37] EP, 2020, p.3, para D.
[38] Sartor, 2020a.
[39] Ibid., p.38.
[40] Ibid. p.45

GDPR as they are relevant to AI, but the present dissertation does not deal with these topics deeply. The common key point is that, once the data is acquired, it is quite difficult, if not possible, to access in or withdraw from the brain of AI systems. As a result of this discussion, one may see that some of the principles and rules vested in the GDPR are not fully exercisable in the case of AI applications.

Furthermore, Sarto's study suggests many policy options, first of all, confirming the application of the GDPR on AI technologies and not putting the businesses in a disadvantageous position during the application, therefore suggesting no urgent change in the GDPR[41], opposite to the early works mentioned above. This dissertation shares the same view as it will be presented in the offered solutions section. However, providing more guidance about the application and introducing soft law instruments by touching to seemingly grey points is suggested[42] which we also came to the same conclusion as a result of our analyses. Another policy option refers to the importance of differing the training data and the data to be involved in the algorithmic assessment. Sartor points the personalized decisions reached by AI and suggests that there should be mechanisms establishing obligations for data controllers to notify the DPAs and ensure their GDPR compliance. While the rest of the options are somewhat mentioned in this dissertation's last part, suggestion regarding the permissibility of repurposing activities with the purpose of scientific and statistical works is a novel one, in our view. Finally, a novel suggestion given by Sartor is related to the assessment of the social impacts of mass data processing by AI which is not addressed anywhere in the GDPR. The scenario analyzed in this dissertation serves a similar aim as it points to the societal impact of AI by evaluating the impact first at the individual level.

The final study to be reported under this title strongly reflects the EP's intention to step forward from the ethics to policy making for AI technologies in general. The study prepared in June 2020 for the STOA[43] reported the issues related only about the heart of the AI technologies (the data) and pointed many principles and rules available, but not easily applicable, in the GDPR. For example, AI technologies were evaluated as they could have such establishments that may cause complexity in understanding, inexplicability and unpredictability hindering the transparency principle which is one of the basic principles data controllers must comply with. Biased and discriminative training data affecting the

[41] Ibid., p.76.
[42] Ibid., p.81
[43] van Wynsbergh, 2020.

outcomes of the AI systems that are very personal was identified as an obstacle before developing ethical AI technologies. The document may be evaluated as the EP's intention of stepping forward from the ethics to policy making for AI technologies in general (also supported with the EC's White Paper detailed below). This study highlights the importance of ethics in evaluating new technology in a particular manner, not in a comprehensive approach as the policy tools do so, as their first aim is to regulate and govern. Ethics, according to the author of the study, is the first step for asking questions in which the answers could lead them in action through policies. This discussion could enlighten the debates around ethics vs. law from a different point of view, but the EC's policy papers point more tendency to the legal regulation than only the ethics.

1.2. The European Commission Policy Papers

The EC's as yet involvement with policy planning towards the regulation of AI technologies resulted in a generation of a significant number of policy papers during the last two years. In 2018, the EC published the EU AI strategy delivering three pillars for AI transformation in the EU: "increasing public and private investments in AI, preparing for socio-economic changes, and ensuring an appropriate ethical and legal framework"[44]. The strategy document could be one way to understand how the EU analyses the differences and similarities, as well as the gap level between the MS in terms of AI readiness. In the pillar of the ethical and legal framework, the AI strategy puts data protection and privacy as a challenge to be tackled. The EU seemed to take the lead in all these three pillars and started establishing the operative aspects of the pillars, for example, the HLEG was created by the EC to receive policy recommendations related to AI regulation, including data protection. The very first and maybe the most significant contribution of the HLEG was to define the term AI[45] according to the EU's perspective which was several times identified as a missing point in the previously mentioned EP works. At the same time, the HLEG published ethics guidelines[46] referring to seven requirements for establishing human-centric AI that is complementary to each other. One of the requirements refers to privacy and data governance and is supported with the other requirements that are directly connected with it such as transparency, fairness, and accountability.

[44] EC, 2018b, p. 1.

[45] HLEGAI, 2019a.

[46] HLEGAI, 2019b.

The AI strategy is accompanied by the European data strategy[47] in which the aim is to carry the EU in a world leader position in terms of data innovation in healthcare, economy, environmental protection, industry, business, education, agriculture, finance, and all the other areas where data drives. To reach this aim, it is clearly stated that the rules and enforcement of the rules should ensure (also) personal data protection. The problems started concerning the data protection specific cases are similar to the ones reported in the EP literature, expectedly. Additional problems were noted, as the lack of standards and tools preventing data subjects to exercise their rights simply together with a lack of data literacy. The strategy gave a clear message that is the current legislation would be soon reviewed in line with the data that is necessary to freely circulate in the EU. The EDPS delivered its opinion on the strategy by supporting this approach, but also by noting the insufficiency of current business-oriented data processing practices limiting the rights and principles such as (and mainly) lawfulness of data processing, purpose limitation, transparency, accountability, data protection by design and by default, and security[48]. Highly related to outcomes of this dissertation, it is important to note that the EDPS supports increasing the digital skills and literacy of the Europeans specific to the data protection literacy increasing the possibility for them to make informed decisions leading their consent to be valid.

The last and one of the most important documents published by the Commission is the White Paper on Artificial Intelligence[49] to launch a debate in the public and in the EU institutions to see how a political consensus could be reached on possible legislation on AI. There is a green light given in the White Paper towards new legislation on AI. It contains policy options around two main ecosystems which are to ensure the trustworthy development of AI in Europe while benefitting from the value of the data excellently. Trust, is strongly highlighted throughout the analysis in the White Paper. It is not only related to Europeans' trust towards the persons behind the AI applications, but it involves all the actors within the chain of trust. These actors are, seemingly, the citizens, the businesses, and the public sector. The document could be understood as the first comprehensive work of the EU identifying the real problems and risks with AI which then will lead the EU institutions towards policymaking. It is also reinforcing the wish of the EU to become a global leader in data economy but without giving up the fundamental rights and European values while doing that. Without a doubt, such a success could be reached collectively, the introduction of national initiatives should be

[47] EC, 2020a.

[48] EDPS, 2020,

[49] EC, 2020.

avoided since they endanger legal certainty (as it may happen with the GDPR), weaken citizen trust, and prevent the emergence of a dynamic European industry[50].

Under the problem definition title, the paper reports the risks for fundamental rights including personal data and privacy protection and non-discrimination in the first place which might be meaningful in the sense that the area needs an urgent regulation or clarification by the view of the EC. The risks are assigned to human oversight, the design of AI, and the autonomous and black-box nature of machine learning that complicates the understandability which then affects the enforcement of the existed rules. Risks regarding the liability regime are particularly addressed in a general approach without assessing the data protection specific issues, however, our opinion is that a specific assessment is needed if new legislation is to fulfill all the missing points. For example, a learning AI system may raise new risks changing the functionality that was not fully foreseen at the beginning of system launch, as we will address further below.

During the reading of the risks for the fundamental rights section, a footnote specific to the GDPR catches the attention in a way that the White Paper points the GDPR's possible weakness in covering the AI-specific risks[51]. It will be the EC's duty to monitor and assess the application of the GDPR on AI technologies, but yet seemingly no tangible case has reached the CJEU making the EC's work hard in this sense.

To tackle these problems, the White Paper points improvement in the legislative framework to address them especially the ones related to the transparency problem, safe operation of AI, the scope of the EU legislation (that may fall short covering the AI-related legislation), dynamic nature of AI systems as a result of ML raising novel risks that were not previously covered in any EU legislation, and the complex responsibility scheme making impossible to implement the legislation and the liability regime. The new legislation will also adopt the risk-based approach like the GDPR, but the EC's position is clear, as it would cover only the high-risk AI applications, leaving the interpretation of the non-high-risk AI-related cases to the existed EU legislation. The concept of the high risk points two cumulative elements: use of AI sectors, such as healthcare, transport, energy, where the risk is significant and/or likely to occur consists of the first element. The second element assesses more particular applications meaning that, as also Article 22 of the GDPR includes if the AI application raises significant (legal) or similarly significant (legal) effect on the individual, it is in the

[50] Ibid., p.2.
[51] Ibid., p.11, supra note 34.

high-risk category. Upcoming parts of the dissertation will clearly prove that Article 22 is certainly applicable to the personal household social robots, too. Seemingly, these points will consist of the main structure of the new regulatory framework planned by the EC[52] which obviously will cover the personal household social robots.

1.3. The EU's Focus Points in Regulating AI

According to the policy papers presented above, specific rules regarding data protection and privacy will form an integrated part of the EU AI legislation. It is easily understandable, that either new legislation will be introduced (which is more probable) or the existed legislation will be brought in line with this technology (or even both approaches will be taken) by the EU law-makers, the risks and problems stated in the policy papers will be the starting points. Overall risks in AI technologies specific to data protection and privacy are:

- AI and robotic applications may cause mass surveillance and profiling that is one of the risks arising from the use of robots at households. A personal home-care robot, for example, may comprehensively collect and process personal data as a result of profiling activity.

- ML techniques enabling AI technologies to perform autonomous decisions, together with profiling, might cause extraction of new information and data about the data subjects which is contrary to the purpose limitation and data minimization rules.

- Specific ML techniques in which, for example, a user's collaboration is needed for learning might affect and change the functionality of the system that cannot be unforeseeable during the system development.

- Technical complexity and the black-box nature of the algorithmic assessments may hinder the transparency and explainability principles.

- Data repurposing, unforeseeable system functionality, transparency and explainability problems, complex data controller and processor relationships, and finally, lack of standards and tools preventing data subjects to exercise their rights may cause ineffective consent implementations, if not impossible to obtain informed and unambiguous consent.

[52] Ibid., p.17.

- Risks during the training of the AI systems might derive from the biased and discriminative data collected that are fed to the algorithms.
- Even though the personal data used for training purposes could be anonymized, there is a strong probability for re-identification of the persons whose data was involved in training data. This is due to AI's ability to extract new meanings to the given new cases.
- Development and operation of AI technologies may involve many actors, from the hardware provider to software developer and maintainer, sometimes even users. When damage is caused as a result of the autonomous action of the robot, this might create even more complex liability scenarios. (based on this-natural person's liability).
- Strict data protection legislation itself may end up with fear for the businesses to develop and implement AI-based tools and services. This may, on the other hand, may encourage businesses to find other ways to solve the liability scenarios. Such scenarios must be pointed not just in a general meaning, but in data protection specific cases.

Until now, we must be able to prove that there is a technology called AI and it is happening even now, with a high probability of rising risks to people's privacy and data protection rights, at least, as identified by the EU. This work aims to analyze the GDPR from the applicability to the household social robots' point of view to bring empirical results which may give a starting point for those efforts put by the EP. The regulation should not be understood only as a legal regulation, in our view; the ongoing solutions offered in the academia for AI technologies (such as ethics by design) are not the purely legal solution. The adopted interdisciplinary approach from the beginning of this study served us to point some different tangible aspects of the defined problems that could be taken into account by not only the legal-AI researchers but also by the social scientists. In the following, the problems subjected to this work, and the methodology to approach these problems will be presented with this interdisciplinary approach.

2. Methodology

"Researchers and engineers in artificial intelligence should take the dual-use nature of their work seriously, allowing misuse-related considerations to influence research priorities and norms, and proactively reaching out to relevant actors when harmful applications are foreseeable."[53]

In general, the aim of legislators during the law-making procedure is to be solving the present legal, social, or practical problems and preventing unwanted future cases. To reach this aim, they first put an effort in creating awareness on the legal problems based on facts and the data at hand and set the legislative agendas following by. Although law-making procedures may follow different paths and they could be affected by different internal or external dynamics, the basic outcome of legislation should not only be related to the current problems, but also the probabilistic future. However, untraceable technological developments bring not only social and cultural challenges, but also legal ones, and neither politicians nor the law-makers could respond to those challenges as fast as the changes occur. Amending a single piece of national law may sometimes take a year, or transformation of a piece of an EU legislation may take some years (as this was the case with the GDPR), but until then, new legal questions may arise which invalidate the effectiveness of the about-to-be-current law. For this reason, 21st-century lawyers should not only deal with the current problems, but also should have an ability to foresee, at least the medium-term future scenarios, so they could prevent possible future problems with the help of the present legal texts. Such an approach is easily observable in the GDPR; the EU lawmaker evaluated the present situation at hand together with the close future scenarios which are very likely to happen, as the articles of the GDPR and several guidelines delivered by the EU agencies point out. However, the rise of AI technologies both in public and in the private sphere has happened so sudden, even the most current data protection legislation, the GDPR, seems to be lacking to answering some of the questions (as will be analyzed in the further chapters) that were previously may not have been thought by the EU legislator. Whether the questions and hypotheses subjected to the analysis of this work have ever been considered by the EU legislator during the GDPR-making (while the answer is negative), due to the volume and content of the documents generated by the EU institutions just now could confirm the existence and the urgency of the case. For this reason, this work adopted a futuristic approach supported by own analysis and by the expert opinions to prepare lawyers as well as lawmakers to foresee and regulate the possible problems regarding data protection in the age of AI technologies in the EU.

[53] Brundage, et. al., 2018, p. 51.

2.1 Motivations Behind the Chosen Methodology

Science and technology develop cumulatively, meaning that, not only the results of the prior researches are of the utmost importance to start a new project, but the problems defined and the methodologies used in previous works could be a useful source for a new project. The same goes for the forecasting methods, as Armstrong stated[54], that any researcher attempting to use forecasting methods should first check the prior works. There are several pieces of literature referred during this work regarding the methodology (see, Scenarios Used in the Legal Literature title), however, one of them presented below is directly related to the topic of this work (robots and law) implementing a well-thought method similar to what we were imagining even before start conducting this research.

Presented at the WeRobot 2019 conference that has been organized since 2012 every year in the US, Ballard and Calo's paper ensured[55] that our work is not a piece of a Science Fiction, but is a way to take guard against the future's possible legal problems of allowing social robots enter in our homes from today. They propose an appropriate method for shaping the Robolaw[56], stating that we could prevent unintended consequences of future legal problems with the help of a foreword thinking way[57]. This way of thinking could be operationalized with forecasting methods that contain several futures research methods that are applicable both qualitatively and quantitatively in legal or social sciences (later, we realized that HRI researchers also use this method frequently). Ballard and Calo applied the design fiction, scenario planning, and the futures wheel methods during their analysis which results could then be translated into qualitative research that could be used as an input by the law-makers. This dissertation considers the design fiction and the scenario planning methods in particular to the hypotheses considered.

2.2. Futures Methods, Law, and Robotics

Ballard and Calo's work definitely is not the only single paper in which this dissertation is based on. The literature review conducted during the course of making this work showed that other similar works are focusing on Robolaw, even more specifically on the data

[54] Armstrong, 2009, p. 2.

[55] Ballard and Calo, 2019, p.3. The paper is referred as "draft" most probably because it is missing only the conclusion part. Otherwise, the implementation of the method, scenarios, and analysis of the scenarios are visibly completed.

[56] This is a term used for robotic legislation. There are other terms being used, such as lex robotica. People who efforts to develop robolaw is called as robot legist or robotist.

[57] Ballard and Calo, 2019, p.3.

protection aspects of robotics, and using these methods properly. They might be few in quantity but they give enough background information to understand the applicability of futures methods in the field of law and robotics. For example, Safeguards in a World of Ambient Intelligence[58] project was based on four (dark) scenarios helping the readers to identify impacts of AI technologies on privacy and data protection. The approach followed in the project was to construct four scenarios each differently based on a specific technology and the risk that it would raise against the right to data protection. In light of the scenarios, the authors questioned the difference between the public and private space in the age of AI technologies, and the role of data protection which is being challenged by the technology. One of the outcomes of the work was pointing the shortcomings of the data protection law specific to the Directive 95/46/EU. This project and the paper gave special attention to transparency, consent, and technology-specific regulation issues with the help of those scenarios.

Another example to be mentioned belongs to Mulligan[59] who conducted a comprehensive investigation of robots' liability through several questions based on a short scenario. In that scenario, a gardening robot capable of learning new behaviors started acting unexpectedly and unforeseeably which left the applicability of the ordinary liability regime out of the scene. Through this small scenario and with the support of the analysis, the author simply pointed out a possible robot liability in a very rational and logical approach with a possible close future case.

A more updated work[60] reporting the EU funded projects ensured the validity of the method in legal sciences, pointing out the fact that the futures methods are known and practiced method in legal sciences. De Andrade collected those projects where scenario-planning also was used to forecast legal challenges arising from technological developments. His work proved, first, that the availability of futures methods for legal planning; and second, he strongly recommended using futures methods for legal research, but especially, during the law-making procedure. Although his paper was not investigating the data protection and robotics topic straight-forwardly, it is an important work reinforcing the idea of the applicability of the futures research method in the legal field.

[58] Ahonen, et al., 2008
[59] Mulligan, 2018, p. 11.
[60] de Andrade, 2012,.338

Effectivity of using futures research methods during the lawmaking procedure aiming at the regulation of technology was proven by Weber, Gudowsky, and Aichholzer[61]. In their work, they particularly implemented a method called technology assessment study in the Austrian Parliament on the topic of Industry 4.0 and concluded that the foresight methods could boost lawmakers to adopt more interdisciplinary and deeper insight for answering technology-related legislation needs.

Present work uses futures methods to help lawmakers to foresee data protection challenges in AI systems which have otherwise never been easy to realize before. In this way, the law-maker could act before an unwanted consequence occur, since once personal data is included in AI systems, it is almost impossible to take (or delete or track) the data back from the system. We think that proactivity embedded in the GDPR should be more enforced, if there will be a revision on the GDPR, and the application of this piece of legislation should also be based on proactivity, too. Further, scenarios and design fiction method will be presented as they were the two methods used in the scientific papers above, and are the specific methods being used in this work, too.

2.3. Scenarios

Scenarios have been used for forecasting and by policy analysis researchers for more than 60 years. It was first introduced in research related to military and strategic planning wok conducted by the RAND Corporation[62]. This method aims to connect present issues with the future through cause and effect links[63]. The intention behind the scenarios is to assist either policy-makers or decision-makers to act now[64] instead of acting later under emergency. This dissertation carries a similar task; to provide some inputs for the EU lawmakers who have been heavily working on shaping the future of data protection legislation challenged by the AI technologies of today and the future.

Futures methods are an integral part of data collection methods for social sciences in a broader sense. The two types of scenarios which are the exploratory and normative scenarios[65] that emerged as a result of the years of practice are proof of this relationship. Introducing a desirable future is the basic aim of the normative scenarios where exploratory

[61] Weber, Gudowsky and Aichholzer, 2019, p. 245.
[62] Glenn and Theodore, 2009, p. 1, Scenarios section.
[63] Ibid.
[64] Ibid. p. 5.
[65] Ibid. p. 6.

scenarios are constructed based on assumptions that may influence one of the several future possibilities. Such assumptions are easy to realize also in the scenario presented in this work.

Building a good scenario requires another methodology and some rules to follow. Three basic rules are pointing to the accuracy and validity of good scenarios, according to the literature. According to that, the first rule points the necessity to start with a plausible (but absolutely should not cause deception[66]) scenario, then ensure the internal consistency of the scenario. Finally, the scenario should be sufficient enough to persuade the policymakers by involving some of the real elements into the case[67]. It is suggested, that from three to six scenarios are sufficient in number[68], but this work will present a whole scenario consisting of several elements and questions, therefore each element could be perceived as a sub-scenario. Since these rules would be vague to conduct a whole Ph.D. research, the following examples under the "Scenarios used in the legal literature" title showed how this method practically was implemented.

A very important aspect of the scenarios is that they acceptably present probable future, but one should bear in mind that the alternative futures are always possible. Therefore, involving experts in the scenario construction was crucial to ensure the representativeness of the scenario in this work. For this reason, face-to-face interviews were conducted with the legal experts to broaden the scope of the scenario which in the end helped to define better and more comprehensive solutions.

2.4. Scenarios used in the legal literature

Scenarios have been used in the broad literature either in robotics or in data protection related works, and sometimes referred even together within a single work. From those, two important papers were identified highly-related to the subject of this dissertation. Carlsen et. al. (2014)[69] focused on the impact of autonomous robots in a society in which they assess the technological impact in the frame of a scenario. The scenario in this work was created in three steps; first, the prototype artifacts for autonomous robots (the artifacts are a service robot placed at malls, a fire-fighter robot, and a household robot for elder-care) were created. This step was followed by creating a hypothetical case applicable to a society based on

[66] Although the purpose of this work is not to design any technical product, an attention was paid to Coulton, Lindley and Akmal's (2016) work which pointed not to cross the line between real reality and the fictionally designed reality.

[67] Glenn and Theodore, p. 11.

[68] Ibid. p.9

[69] Carlsen, H. et al., 2014, p. 97.

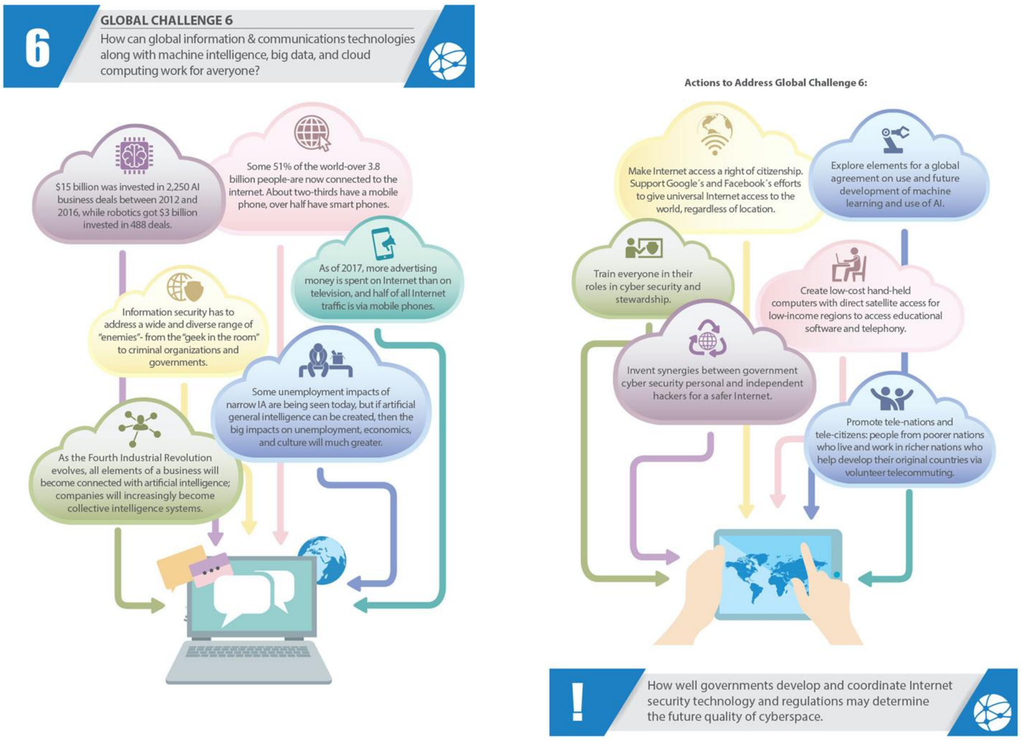
ethical and practical questions gathered out of those artifacts. Finally, society's reactions to the questions were also measured. A multi-dimensional debate that the paper further put was based, firstly, on the robot's capabilities which pave the way for extensive surveillance at homes and in public spaces. Another debate focused on the rights and conflicts from the aspects of replacing human force from the job market point of view. Finally, each debate was framed within the ethical discussions. In this way, the authors could define two types of groups in society according to their scenario interpretations[70]: a skeptical society who wishes to control technology at any level, and a technology positive society who is liberal and approaches the robotic technologies with few restrictions. The scenario prepared in this dissertation shows many similarities with Carlsen et. al.'s work from several aspects. For example, it captures an artifact from the literature (personal household robot), then raises a hypothetical case that was created based on the current discussions in the legal literature (our scenario), and completes it with our analysis together with the interpretation of the expert views.

The second paper related to the subject area of this dissertation belongs to Minkkinen who stated that lack of foresight methods in the policy-making process may cause a lack of future consciousness in the real policy.[71] Minkkinen proposed a new futuristic privacy model shaped by an institutional approach which, according to the study, should be based on the dynamics in understanding the privacy and historical processes. These processes should be defined based on the cultural norms and instruments as well as technology. A complete model that Minkkinen reached had presented an entire scenario, specific focus to the Right to be Forgotten as an example. Comparing the GDPR and the Finnish interpretation of the GDPR in the field of security showed that the foresight element was missing in making the GDPR process since the EU lawmaker focused only on responding to the past and present challenges, not the future ones. Minkkinen stated that the EU lawmaker did not even discuss the future challenges.[72] One aim of this thesis is to prove how the legal experts evaluate the same futuristic scenario differently even though the legal framework subjected to the interpretation is supposed to be the same. Therefore, the lack of unique interpretation in real cases may challenge the GDPR's unified approach.

[70] Ibid., p. 98.
[71] Minkkinen, 2015, p. 2.
[72] Ibid., p. 5.

Besides the two works presented above, a mention must be made on “The Millennium Project”[73] in which almost all the futures research methodologies have been used for forecasting several issues including the legal ones. In this ongoing project, 15 global challenges were defined based on a comprehensive evaluation of current problems and insightful solutions raised by more than 4.000 experts for future problems. Technology-related questions are always a part of each scenario. The project refers to a few privacy related questions under the Global Challenge 6 presented in Figure 2., but the approach followed is much more comprehensive as it could be observable in the figure.

A comprehensive investigation conducted in the literature proved that scenario planning in a Ph.D. work focusing on legal questions could be a sufficient method. To present a full scenario, the design fiction method was used in this for work data collection method.



6 GLOBAL CHALLENGE 6

How can global information & communications technologies along with machine intelligence, big data, and cloud computing work for averyone?

$15 billion was invested in 2,250 AI business deals between 2012 and 2016, while robotics got $3 billion invested in 488 deals.

Some 51% of the world-over 3.8 billion people-are now connected to the internet. About two-thirds have a mobile phone, over half have smart phones.

As of 2017, more advertising money is spent on Internet than on television, and half of all Internet traffic is via mobile phones.

Information security has to address a wide and diverse range of “enemies”- from the “geek in the room” to criminal organizations and governments.

Some unemployment impacts of narrow IA are being seen today, but if artificial general intelligence can be created, then the big impacts on unemployment, economics, and culture will much greater.

As the Fourth Industrial Revolution evolves, all elements of a business will become connected with artificial intelligence; companies will increasingly become collective intelligence systems.

Actions to Address Global Challenge 6:

Make Internet access a right of citizenship. Support Google´s and Facebook´s efforts to give universal Internet access to the world, regardless of location.

Explore elements for a global agreement on use and future development of machine learning and use of AI.

Train everyone in their roles in cyber security and stewardship.

Create low-cost hand-held computers with direct satellite access for low-income regions to access educational software and telephony.

Invent synergies between government cyber security personal and independent hackers for a safer Internet.

Promote tele-nations and tele-citizens: people from poorer nations who live and work in richer nations who help develop their original countries via volunteer telecommuting.

! How well governments develop and coordinate Internet security technology and regulations may determine the future quality of cyberspace.

Figure 2. The Millennium Project Global Challenge 6
How can global information & communications technologies along with machine intelligence, big data, and cloud computing work for everyone?
Source: http://www.millennium-project.org/challenge

[73] Official website of the program is accessible here: http://www.millennium-project.org/ Last accessed: 20 January 2020.

2.5. Design Fiction

“Compared with the world just 20 years ago, we take a lot of things for granted that used to be the stuff of science fiction. Clearly, much can change in just two decades.”[74]

Design fiction is, as the term’s father Bruce Sterling describes, “deliberate use of diegetic prototypes to suspend disbelief about change.”[75] It contains the word fiction because it aims to present the other worlds that are different from the usual ones; the people whose lives are different from ours.[76] It focuses on a particular element, not using a prediction way, but raises questions to discover the future, based on present implications.[77] Pieces of each design fiction present a range of causality and cumulative events that follow one after another.[78] It is a scientific research method that has been used by academic scholars aiming to put a clear picture of the future for further and deeper analysis.

Often, Science Fiction and design fiction are mixed and it is claimed that Sci-Fi is not an appropriate method for conducting an academic research. If so, the distinction (if there is any) should be mentioned to answer possible questions regarding the scientific validity of this method used in the present work. Science Fiction indeed used to be a part of the entertainment world mostly, and design fiction is a scientific method. However, today, items are shown as part of Sci-Fi literature evidentially become real, and become an ideal tool for the industry, as Dourish and Bell[79] proved. The relationship between scientific researches and the Sci-Fi has evolved in a way the former comes after the latter and in this relationship, there is no space for evaluation of consequences of such technological developments on culture or power of states[80]. What the authors propose as a solution is about using fictional design to prevent undesirable consequences of technology’s effects. Besides Dourish and Bell’s work, there are other examples indirectly referring to the design fiction literature presenting technology’s effects on individuals’ lives.[81] Julian Bleecker, a team member of the Near Future Laboratory where design fictions are turned out to be a prototype in the

[74] Microsoft, 2018, p.3.

[75] Sterling B. (2013) ‘Fantasy Prototypes and Real Disruption’, [Online], Keynote-NEXT, Berlin, http://www.youtube.com/watch?v=2VIoRYPZk68.

[76] Blythe, 2017, p. 5400.

[77] Wong, Merrill and Chuang, 2018, p. 1360

[78] Blythe, 2017, p. 5402.

[79] Dourish and Bell, 2014, p. 774.

[80] Ibid, p. 776.

[81] Coulton, Lindley, and Akmal, 2020, p. 20.
These works do not present scenarios but evaluate them to contribute design fiction literature, methodologies, to do and do not dos, but the scenarios the authors present considered in this work.

industry says, that “the science happens in between the fact and the fiction”[82], pointing out the fact that it may not always easy to observe the difference between the real science and the fictional one[83]. Design fiction scenarios are written in the present tense because they present things that are in the process of becoming and the scenario is a part of this process; it has some degree of reality[84]. Turing’s question was maybe more a topic of Sci-fi in the ’50s, but then when engineers gathered much more knowledge to answer Turing’s question in the ’80s, it was one step further than fiction. This relation between Sci-Fi and design fiction gave us a margin of creativity within the borders of reality.

The design fiction method is heavily used in different law-related fields, such as ethics. The famous Trolley Problem[85] is based on design fiction which today is a topic of a legal discussion (the legal liability of robots), especially, in scope of the self-driving cars. In such ethical discussions, the question to be placed is generally “what people should do”[86], but the present dissertation is questioning how the law should give answers to the particular fictional scenarios. This question is related to legal design which provides ex-ante design framework together with the quality in rulemaking standards assessing the impact of a piece of legislation proactively[87] that is also strongly referred in the GDPR. One of the novelties of the GDPR is Article 25 emphasizing the system design and interpretation of the right to data protection together based on fictional assumptions. The philosophy behind Article 25 is to first imagine such systems that would be data protection-friendly, and then turn it into a product that ensures GDPR compatibility. Based on all practices that exist in the literature and on Article 25 of the GDPR, the design fiction method is a sufficient method to analyze the questions referred to in this work.

2.6. Scenario Design

The designed scenario in this work is a result of a comprehensive literature review on AI and law. After understanding the main problems referred to in legal academia regarding the

[82] Bleecker, 2009, p. 27.
[83] Ibid., p. 29.
[84] Blythe, 2009, p. 7.
[85] One of the best visual explanation on what the trolley problem is presented in the MIT’s Moral Machine game where the players should decide instead of a self-driving car in certain accidental situations. See: http://moralmachine.mit.edu Last accessed: 25 January 2020.
[86] Baumer, E. P. S. et al., 2018, p. 19.
[87] EC has a “better regulation toolbox” guiding the EU Institutions (but not limited to) on how to conduct an impact assessment of a particular EU legislation. See: https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en Last accessed: 25 January 2020.

use of AI technologies, the focus was made on the data protection topic specifically. Reading the GDPR, the case-law of the CJEU and the legal and technical literature helped us to raise new questions open for an interpretation and a debate with the experts. Questions referred to the experts could be found in the Appendix. Since AI technologies have a broad definition, case of social robots were chosen and was reviewed both in academic and industrial point of views. Once the initial scenario was ready, it was shared with seven scholars[88] for their evaluation based on a conversation[89]. When the scenario reached its last draft, it was once again shared with the experts for their approval. Once they approved, the scenario was ready to be presented to the interviewees. During the interviews, the validity and reliability of the scenario were ensured with Questions number 1 to 3 in the Appendix.

2.7. Expert Interviews

To ensure the validity of the fictional case and to collect data, this work practices also interview method[90] which is one of the research methods often used in legal sciences. Conversations were conducted with 15 experts from the four EU MS, specifically, from Finland, Hungary, Italy, and the Netherlands. These four countries are chosen as a sample 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 countries. Since the GDPR is a regulation and should be applied in every EU MS in the same way, no criteria were defined for the sampling method for legal research. Furthermore, these countries' AI readiness Index 2017 (the year that we chose the topic for the Ph.D. research) was the last criterion taken into account for choosing the sample countries[91]. After choosing the location, the following criteria were identified when choosing the experts who:

[88] The author would like to thank to Attila Kertész, Anton Gradisek, Akif Berber, Bedrettin Gürcan, Dr. Marton Sulyok, Dr. Szilvia Váradi, Martijn van Otterlo, Prof. Gordon Hunter and Zsuzsanna Mátrai for their contributions to develop the ideas in this scenario. Further, the following resources provided some other ideas while developing the scenario: Wright, et. al., 2014; EC, 2015; Rhoen and Yi Feng, 2018; Talty, 2018 (web resource); National Research Council, 2012. Special thanks to the organizers as well as the lecturers of the Interdisciplinary Summer School on Privacy organized in 2018 in Nijmegen for introducing me the scenarios as a scientific research tool.

[89] This technique is called as a strategic conversation. Ratcliffe, 2002, p. 23.

[90] Watkins and Burton, 2013, p. 67.

[91] This index is being prepared by the Oxford Insights measuring the government's readiness on AI technologies from several aspects indicated in the policy papers of each country in the world. Criteria the index is referring to are collected under three main titles: governments' public service reform plans, economy and skills, and digital infrastructure. Measurements are made on the data collected from several resources, such as the Global Innovation Index, UN e-Government survey, World Bank, and OECD. See: https://www.oxfordinsights.com/government-ai-readiness-index Last accessed: 20 October 2019.
A note should be made here about the fact that AI Readiness Index 2019 reflects some differences among the countries subjected to this research compared to the same index made in 2017. For example, while it was the Netherlands leading in Western Europe in 2017, now it is Germany took over in 2019. Hungary stepped down

- Currently work at a law firm or an institution taking a role in the implementation or interpretation of the GDPR (DPAs),
- Have experiences regarding the application of the GDPR,
- Have a professional interest in AI technologies (e.g. published a paper, gave a speech, analyzed a legal case),
- Have indicated to be a part of this work.

Contacting the experts was possible via the personal network, also suggested as the right approach in the literature[92]. After contacting each expert, a series of visits were made to these countries to conduct the interviews. All interviews were conducted face-to-face to ensure the clarity of the scenario. The interview questions were prepared and sent to the experts beforehand leaving some time for the experts to carefully read them and ask back in case of unclarity. This act also allowed raising some new questions, paving a new way of pointing to new aspects of the scenario. The interview questionnaire could be found in the Appendix.

The interviews gave the insight to see what are the differences between the expert opinions and from what major ways they approach the scenario. This is important from several aspects: when a case is brought, for example, before the CJEU, individual judges' opinions mostly guide the interpretation of that case. There might be many reasons behind judges' decisions; from individual to cultural, to professional practices gained as a result of experiences and so on. Therefore, expecting judges' consensus for the same case not only in different countries but even within the country is not a realistic view. Seeing how opinions of the experts differ or get closer to interpreting the same case within the same legal framework (GDPR) helps to improve the interpretation of legal documents. For this reason, we first gave our own evaluation based on the available data (CJEU cases) and then asked for the expert opinions' on the questions deriving from our interpretation. Expert opinions were evaluated as another group of data besides the CJEU data we interpreted.

from its position for two years. While Finland is stable in its leading position in Northern Europe, Italy stepped up among the Southern European countries. However, as it is early observable, none of these changes are that large to affect the research design in this work.

[92] Watkins and Burton, 2013, p. 75.

3. Data Evaluation

Several recommendations and principles are drafted in academia on how to find the best method for analyzing the different types of data. According to that, the very first step is to analyze the data at hand to determine to apply qualitative or quantitative methods, or mixed of both, to certain research. While quantitative methods may seem more favorable than the qualitative ones by academia, a condition for applying a quantitative method depends mostly on the availability of data[93]. Although quantitative methods could be applied also in the legal field, for instance, to help policymakers to understand society's approach to the robotics field[94], since personal robots have not yet been appeared at households, it is safe to say, that we are lack of a quantitative data. Existed case law and the guidelines cover some of the questions covered in this work and they will already be presented in the further sections.

A comparative approach adopted on analyzing the experts' opinions influencing their decision-making[95] helped us to experience their worlds and critiques[96] which represent a part of their legal culture. Many discussions referred in legal research methods on determining whether to focus on the similarities or to the differences between the legal systems (or expert interpretations, in the present case) is better than the other[97], however, this work is eligible to focus on both. Both the similarities and the differences among the expert opinions will be presented through this work, based on causal and action models. The causal approach assumes the interrelations between one phenomenon to another (e.g. GDPR-technology relationship) where the action approach focuses on the individual behaviors (experts' opinions on the jury process)[98]. The comparative method in this work is scientific (or a theoretic) one, rather than a legislative one[99], meaning that there is no doctrinal analysis made during this research since the focus is on the applicability of certain legislation on futuristic technology, rather than focusing on how the legislation was made.

4. Literature review

The literature used in this work is largely citing the primary scientific resources with a special focus on evaluating personal data protection legislation on algorithms, Artificial

[93] Armstrong, 2009, p.7.
[94] Mejia and Kajikawa, 2019, p. 121.
[95] Watkins and Burton, p. 124.
[96] Gonzatto, R. F. et al., 2013, p. 38.
[97] Watkins and Burton, 2013, section 6.
[98] Watkins and Burton, p.139-140.
[99] Lomio, Wilson and Spang-Hanssen, 2011, p.60.

Intelligence, and robotics, especially, social robots. Further, documents generated by the EU, and the documents generated by the public institutions, private companies, and NGOs available in the sampling countries reviewed, to estimate in what level the countries are being prepared for regulating those questions raised in the literature. These documents also lead to raising new questions and forming new hypotheses before the actual analysis was made.

Several online databases, namely, HeinOnline, ACM Digital Library, IEEE Xplore, EBSCO Academic, Wiley Online Library, CURIA, Springer, Taylor and Francis, were searched to reach to the primary resources. Reports generated by the industry, namely, Google, Microsoft, IBM, and Facebook were also reviewed. Specific resources, such as, International Data Privacy Law, European Data Protection Law Review, Computer Law and Security Review, CJEU decisions and Advocate Generals' opinions, Foresight, IEEE magazines, Eurobarometer works, International Journal of Social Robotics, AI and Society, Futures. Article 29 Working Party guidelines and EDPS websites were reviewed every month. Keywords used in searching the documents were: data protection, consent, transparency, privacy, GDPR, AI and law, social robots, data protection, and robots. Refining options offered in the databases were used to limit the scope and year of publication. Special attention was given on the publications made by the time of GDPR making and after it entered into force. Regarding AI and law literature, we realized that it is a phenomenon of the last 5 years, so we set the publication year in line with it.

5. Contribution to the Scientific Field

A novelty of this dissertation is vested on testing a social robot's legal consequences precisely on data protection which has not yet been examined in academia[100]. The success of the work, in our view, is that its ability to bring both future and legal questions together which reduces the complex issues to a practice that could be easy to understand. It also brings a tangible roadmap to deal with the questions referred within academia. Through the analysis made here, we aim to show possible practical challenges that may occur in case of data protection in the future, if no action is taken today. This work invites European lawmakers to evaluate the current data protection legislation from a concrete perspective represented in this work.

[100] During this study, we found no research testing a theoretical legal case involving social robots and testing the consequences from the personal data protection point of view.

The output of the present dissertation, hopefully, could be an input for designing a better data protection framework related to AI in the EU, since the law is also about design, and creativity in legal thinking which could be presented in the well-designed scenario could lead to making a future-oriented, a techno-ready law.

II. Right to Data Protection

Peter Sondergaard, former senior vice president of Gartner Inc., once said that: “Big Data is the Big Oil of the 21st century”[101]. What makes data valuable is not meaningful when it is standalone, but the meaningful expressions it gives once it is combined with other data. Accessing ready information is an easy task, but carving out information from a restricted resource neither is time friendly nor guarantees accuracy. After the information explosion following the Second World War, information became power with the help of technological developments and advanced electronic systems making it easy to acquire data on the specific field or even to someone specific, paving the way to get them to know, even better than themselves.

Right to data protection originally derives from the right to privacy which the terms today are still related, but also distinct at the same time. For example, there are scholars naming data protection as information privacy, which is a typology of privacy literature[102]. This work focuses more on data protection than the right to privacy, based on the data processing capabilities of the current technology since it is not possible to *process* privacy. Once profiling and surveillance technologies entered in homes[103] (e.g. via smartphones or a social robot), data protection becomes both broader and more specific from the right to privacy[104]. In a broader sense, and on one hand, the right to data protection is closely related to the other fundamental rights, such as freedom of expression[105]. On the other hand, data protection is more specific than the other fundamental rights, since it applies only to those cases where personal data is processed.

The case-law of the two European courts complicated this distinction for some time when the ECtHR interpreted privacy in a broad meaning that is involving data protection. And the CJEU interpreted the right to privacy and the right to data protection separately[106]. The ECtHR, interpreted the right to privacy comprehensively as it could include the right to data protection as well, but it does not have to include all information on identified or identifiable

[101] “Big Data Fades to the Algorithm Economy”. Peter Sondergaard, [Online], Forbes, Accessed from: https://www.forbes.com/sites/gartnergroup/2015/08/14/big-data-fades-to-the-algorithm-economy/ Last accessed: 2 Febraury 2020.
[102] Koops, et. al., 2017, p. 484. The authors identified eight types of privacy, namely, bodily, intellectual, spatial, decisional, communicational, associational, proprietary, behavioral privacy, and informational privacy which is a new type of privacy.
[103] Wright and Raab, 2014, p. 278.
[104] Gutwirth and Hildebrant, 2010, p. 37.
[105] Freedom of expression is one of those exemptions referred both in Directive 95 and in the GDPR.
[106] Gellert and Gutwirth, 2013, p. 524.

persons separately, as the CJEU does. Technology, specifically the AI effect slightly melted this distinction in this sense. Recently, the ECtHR put a borderline between the right to data protection and privacy in the case regarding content personalization used for election propaganda named as algorithmic governance (even though indicated that the data protection right is a "governance mechanism to safeguard the privacy and other rights"[107]). In any case, the right to data protection is protected under both jurisdictions[108].

To our view, the distinction should be made and is necessary, because the EU has legislation specific to right to data protection (Directive 95/46/EC and now the GDPR), and the MS established authorities specific to safeguard it. When the two jurisdictions are such engaged to each other (e.g., all the EU MS must be the signatory country to the ECHR), such a distinction may restrict the broader interpretation of the cases.

The distinction between the right to data protection and privacy has a historical fact, to our view. The protection of privacy as an essential human right has been entrusted in several regulatory texts, most of them entered into force after the Second World War. The reason behind this fact is that, the way of the use of personal data by political powers to "segregate populations, target minority groups and facilitate genocide"[109]. Since then, the way of collection and use of personal data has much changed with technology but the fact with the misuse of personal data is not much changed. Today, there is less need for eavesdroppers to predict who belongs to what type of political or religious group, thanks to the digital personality the people create by themselves and to the algorithms analyzing these profiles. Such profiles accelerate algorithms to predict, for example, that an individual belongs to a certain religious group with 82% probability[110]. While a credit card number is personal data, unless it gives information on the person's private life such as shopping behavior, it cannot be easily considered under the scope of privacy protection. Even though it gives information about the person's shopping behavior, the GDPR is in favor of interpreting this information as personal data rather than privacy (as Article 22 of the GDPR points so). The right to privacy alone does not enable the person subjected to a right to access his data[111] which is one of the basic rights included in any data protection legislation in Europe. Furthermore, principles such as transparency and fair processing, together with the existence of independent supervisory authorities again specific to the protection of personal data, not for

[107] CoE, 2017, p.20.
[108] Kokott and Sobotta, 2014, p. 228.
[109] Robinson, N. et al., 2009, p.6.
[110] Kosinski, Stillwell and Graepel, 2013, p. 5803.
[111] Mostert, M. et al., 2017, p. 6.

the right to privacy[112]. Such fundamental differences make it easy to understand the distinctive characteristics of the two fundamental rights recognized in European countries and the rest of the world.

The value of personal data is vested in its ability to give clues about a person's specific information which makes the traditional understanding of privacy distinct from practical, but also the legal point of view. To present how the right to data protection has been evolved in a legal sense, we need to first take a look at its historical roots in legislation.

1. Right to Data Protection in International and European Law

The UDHR and the ECHR historically are the first international legal documents preparing the legal construction of the right to data protection. As mentioned before, data protection right in the form of right to privacy was first expressed in the UDHR in the Article 12, as follows: “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." Although the UN took the first step towards the protection of human rights, it would not be wrong to say that right to data protection has distinctly developed in Europe. Article 8 of the ECHR ensures the right to respect for private and family life, home, and correspondence which scope has been expanded to the right to data protection, to access personal information including health-related information, pictures, photos, and images during the years of interpretation[113].

In addition to the UDHR and ECHR, the OECD[114] and APEC[115] published some soft law instruments on the protection of personal privacy. These documents are not considered legal documents based on their guideline nature. However, they are still considered to be important international documents protecting the right to privacy.

Currently, neither the UDHR nor ECHR does not refer to the right to data protection as a separate right, as mentioned before, but the Convention 108 itself is one of the instruments of the CoE specifically designed to protect the right to data protection and is the first international legal document protects personal data separate than privacy. It has quite a large

[112] Ibid, p.8

[113] European Court of Human Rights Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home, and correspondence Updated on 31 August 2019.

[114] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. Updated once and only in 2013.

[115] APEC Privacy Framework was adopted in 2004 and APEC Cross-Border Privacy Rules System was launched in 2011, then updated in 2015 upon the updates made on the OECD guidelines.

number of signatory countries; all the 47 members of the COE ratified the Convention, 9 non-CoE member countries signed and ratified (Argentina, Cabo Verde, Mauritius, Morocco, Mexico, Senegal, Tunisia, Uruguay) the Convention. The document was last time updated in 2018[116] very likely in line with the GDPR (e.g. unambiguous consent was added in the legal text).

Convention 108 was the only European international treaty before the Directive 95/EU/45. It drew the rules for safeguarding the right to data protection, aiming to bring minimum standards for the protection of personal data, so the countries are free to adopt more or better solutions in their jurisdiction. In this way, it prepared the basis of most of the principles further improved in the Directive 95/46/EC.

Last but not least, the relationship between the Convention 108 and the GDPR worth noting in this work. The organic relationship between the GDPR and the Convention 108, at least, from the points that this work focuses on, does appear in multiple ways. There is no doubt that they influence each other in some ways. For example, one of the updates inserted in the Convention after the GDPR is the consent mechanism. Convention uses exact GDPR statements such as in Article 6 of the Convention as "unambiguous consent" and extends the definition of personal data to be included biometric and genetic data. The rights of data subjects were extended to the automated decision-making rule as of the GDPR. The principle of transparency is now in the center of the Convention. DPIA and DPbD rules are inserted in the Convention in Article 10. Even though the organic relationship goes at some level on, the EU's data protection legislation offers much more specific rights, rules, and obligations to the right to data protection.

2. Right to Data Protection in the European Union

The development of the right to data protection in the EU first shall be mentioned at the level of specific MS' legislation. Even though the first national privacy legislation was adopted in the US in 1974[117], the ECHR might have been influential on the national data protection legislation explosion *i*n Europe in terms of individual European states. For example, the first domestic data protection law entered into force in 1970 in the Land of Hessen, Germany,

[116] It was updated in 2001 for the first time bringing the obligations to the states to ensure an adequate level of protection in trans-border data exchanges and several additional safeguards to apply at domestic law, such as the establishment of a national data protection authority.

[117] Küzeci, 2010, p. 120.

just ten years later than the enactment of the ECHR[118]. The citizens of Hessen realized the risks for their data (e.g. storing without an indication on purpose limitation) being stored in the central federal database without a legal basis. Following the Hessen example, many other states in Germany adopted a data protection legislation. Adoption of a German Federal Data Protection Act (Bundesdatenschutzgesetz) in 1977 then became the first national data protection law in Europe. Sweden followed the German example and adopted a data protection legislation in 1978. Other European countries immediately (except Ireland, UK, and Italy) adopted the right to data protection at their constitutions and started preparing their legislation by that. Once the Directive 95/46/EC entered into force, all MS was abided by standard general rules leaving a large margin for national interpretation.

3. Directive 95/46/EC

Ensuring the free movement of data that could protect and enhance the single market became a crucial principle for the EU during the transition period leading to economic union. Following the German data protection legislation, the MS adopting divergent approaches to the protection of the right to data protection in the EU was evaluated as a threat to the EU's internal market.[119] Directive 95/46/EC brought relatively a common ground to those very different legislative practices by introducing standard rules. First of all, it covered many issues mostly related to data breaches rather than privacy. By stating data breaches and with the support of the e-Privacy Directive[120], the EU legislation could ensure the protection of the right to privacy and data protection without leaving a gap between. Next, it would not be wrong to state that the Directive 95/46/EC brought fairly stronger legal protection than the other international documents, such as the OECD guidelines, because it introduced many rights that could be counted new in this field. Hence, it is not a guideline but is a legally binding document providing stronger and enforceable protection for the citizens. The right to obtain source of the information, the right to request data modification, consent rule, variety of remedies, and comprehensive rules for personal data transfers abroad could be presented as examples. Later, the case-law of the CJEU[121] developed the interpretation of

[118] Ibid., p. 117.

[119] Hoofnagle, van der Sloot, and Borgesius, 2019, p.70.
The preamble of the Directive, seventh incident.

[120] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002, p. 37–47.

[121] C-131/12 - Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD), Judgement of the Court, [2014], ECLI:EU:C:2014:317.

the Directive 95/46/EC by introducing new rights (e.g., right to erasure, known as the Right to be Forgotten in the GDPR) and also expanded the scope of the definition of personal data (e.g., cookie and IP decisions).

There is no doubt that the Directive 95/46/EC was playing a key role in the adoption of the right to data protection within the Charter of Fundamental Rights in 2000, which became legally binding documents in 2009 when the Lisbon Treaty entered into force. Article 8 of the Charter ensures personal data protection similar to Article 8 of the ECHR, Directive 95/46/EC, and Convention 108. However, Charter does not specify principles as detailed as the Directive 95/46/EC which differs the two legislation from each other. After the Lisbon Treaty, the Charter made the same effect as the other EU Founding Treaties which means Article 8 regulating the principle of consent, purpose limitation, and legal basis for processing to become directly binding rules for the EU institutions. In the famous Schrems case[122] as well as in the other cases[123], the CJEU was referred to cases related to the application of Article 8 of the Charter, instead of proving the importance of inserting right to data protection in implementation and interpretation of the GDPR[124].

Directive 95/46/EC inspired many other countries outside of the EU. For example, the Turkish Data Protection Law was drafted with similar rules to Directive 95/46/EC [125] as the other candidate countries such as Serbia. However, as will be presented below, there was still a lot to do to bring the EU data protection rules to be the most beneficial level on the economic and political sense. The GDPR was drafted in such an environment and first of all, we would like to clarify the concept of regulation as an EU legal instrument to understand why the GDPR made great repercussions both within the EU and globally.

Once again, a note could be left here on to the discussions about the relationship between the right to privacy and data protection, that when the GDPR entered into force, EU's strong

[122] Case C-362/14 Maximillian Schrems v Data Protection Commissioner, Judgement of the Court, [2015], ECLI:EU:C:2015:650

[123] Case C-203/15 Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, [2016] Judgement of the Court ECLI:EU:C:2016:970. Application of a national law were three UK nationals whose traffic and location data was requested by the Swedish Telecom Authority, from Secretary of State for the Home Department of the UK and Northern Ireland referred the case for preliminary ruling asking whether the national law allowing their data transfer contradicts with the Article 8 of the Charter.
Joined Cases C-141/12 and C-372/12 YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel, Minister voor Immigratie, Integratie en Asiel (C-372/12) [2014] Judgement of the Court, ECLI:EU:C:2014:2081 scope of the Article 8(2) where "right to access" is given to everybody was limited to only those data concerning the data subject rather any other data generated during application for residence permit and those personal data should fully be made available to the data subject in an intelligible form.

[124] Mostert, M. et al., 2017, p. 17.

[125] Gültekin Várkonyi, 2017a, p. 239.

data protection rules separated the right to privacy, unlikely the other European and international legislation providing a legal basis for the right to privacy and data protection together. Replacing traditionally known privacy by design and by default principle to the data protection by design and by default is one of the shreds of evidence of this statement. Although these terms were missing in Directive 95/46/EC, it was still the largest milestone in the EU data protection legislation history.

4. The General Data Protection Regulation and the Novelties

The EU legislator did not overlook the changes in the society triggered by technology and did not ignore the fact that every legal document once should be updated to find solutions to the new-born societal problems. Schrems and Google Spain cases showed that the EU shall have a unified data protection legislation triggering a harmonized position enhanced with the safeguards against the foreign tech-giants. The EDPS' opinion on the necessity for adopting a data protection Regulation spells out the reasons behind the GDPR[126], as follows:

1. Technological changes; which refer to the fact that the technology is not the same with the time when Directive 95/46/EC was enforced and of today.
2. Legal certainty; which refers to the EU's ambition on enforcing more effective and efficient rules on the MS rather than formalities.
3. Harmonization; which refers to the power of regulation as an EU legal document.
4. Finally, and the most significant in our view, is the protection of EU citizens' data towards third countries (e.g. where the Big-Tech companies are located) based on adequate rules.

Obviously, switch from the Directive to Regulation is the most remarkable change in EU data protection legislation, however, there are other novelties the GDPR brought, especially for the data subjects' rights point of view. Before presenting the novelties of the GDPR, that are related to the present work's research field, we would like to open up the meaning of the term harmonization, the adequate rules, and the effect of technological changes affected the GDPR's made, as the EDPS' opinion referred.

[126] EDPS, 2012, pp. 2-3.

4.1. Regulations as Part of the EU Legal Structure

Treaties are the primary resources establishing the EU and defining the share of competences between the MS and the EU. After the Treaties, Directives and Regulations are the only legal documents with the effect of directly applicable, almost as strong as the Treaties, meaning that they also have a direct impact. Article 189 of the EEC affirmatively indicates that "Regulations shall have a general application. They shall be binding in every respect and directly applicable in each Member State". Article 288 of the TFEU confirms this rule once again by stating that, "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States." Case law of the CJEU has been reinforcing these rules with its decisions preventing the MS from applying the regulations partially or lately since the earlier years. For example, in a case referred to the CJEU[127], the CJEU reinforced the Article 189 of the EEC and indicated that "by reason of their nature and their function in the system of the sources of Community Law, Regulations have direct effect" and Regulations "prevent the implementation of any legislative measure, even if it is enacted subsequently, which is incompatible with its provisions"[128]. In another case,[129] the CJEU drew the attention to the fact that a MS cannot opt-out Regulation provisions which are effective from the date they were published in the Official Journal. MS must follow the transition periods since regulations are fully applicable to the MS (in general, the obligations, prohibitions, duty of ensuring rights of individuals), however, there is no monitoring instrument of the EU to check whether MS is in full compliance with Regulations at any date.[130] The cases are evidential on the power of the regulations in the EU legal system, leaving no margin for a national interpretation, and even no exception for the implementation date.

Directives are also important to secure uniformity of the EU law but gives a large margin of appreciation for implementing the general rules. Its initial purpose is to harmonize the EU

[127] Case 43-71 Politi s.a.s. v Ministry for Finance of the Italian Republic, [1971], Judgment of the Court, Case no 61971J0043.

[128] Ibid, p. 1048-1049, para. 9.

[129] Case 39-72, Commission of the European Communities v Italian Republic. Premiums for slaughtering cows [1973] Judgment of the Court, ECLI:EU:C:1973:13, para. 8.

[130] Indeed, Commission could monitor the MS' status whether they are fully ready to implement Regulations, but first, the Commission needs a well-grounded suspicion towards a MS, then it needs a legal case to refer to the CJEU, and finally, it is practically impossible to check each and every MS in a daily basis whenever a Regulation or any other legal instrument was followed.

law, but certainly not unification which is the ultimate aim of Regulations[131]. This is the basic difference between the two legislative documents in the EU legal structure. Reflection of this difference practically serves to the aim that, when the Directive 95/46/EC was in force, there used to be 28 different ways of different implementation regarding the right to data protection. For example, Germany and Austria (two historically privacy-sensitive countries) are known for their stricter data protection regimes compare to Ireland, Italy, and Romania (so to say, the countries having more liberal economy incentives). Indeed, it is not a surprise that the European headquarters of some of the tech giants (Facebook, Google) were all settled in Ireland. Most of the MS was not taking the right to data protection into their political discussions, so the awareness regarding the data protection issues was low[132]. Although it has never been brought to any court (either at MS national courts or to the CJEU) there was a clear imbalance between the level of protection of the personal data of the individuals located in different MS. The GDPR eliminated these different implementations both within the EU and uniform a consistant data protection mechanism towards the rest of the world.

4.2. Territorial Scope

Article 3 of the GDPR ensures the applicability of the GDPR to the controllers regardless of their establishment in the territory of the EU. The scope of such processing applies to the data controllers offering goods or services (either is a free service or subject to a price) to the data subjects and more specifically, monitoring the data subjects' behaviors. There are legal, but also practical reasons for defining the territorial scope of the GDPR in this sense.

Until the American privacy activist and the former NSA employee Edward Snowden made the historical revelations in 2013, no international data protection crisis appeared. Snowden reported that the NSA and, naturally, the United States had been 'spying' personal digital information via Internet and phone companies to monitor people all over the world as well as the countries (as Brazil and India)[133] under the data processing for counter-terrorism purpose. It is also known that the American law enforcement authorities collected personal data of not just their citizens, but others including EU citizens from private companies such

[131] Article 288 of the TFEU states that: "A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods".

[132] Custers, et. al.. 2018, p. 238.

[133] Farrell and Newman, 2016, p.130.
Giles, 2015, p.544.

as Google for several types of investigations[134]. The EU and the US many times found themselves in political conflicts[135] caused by the distinctive approaches to the right to data protection[136]. Snowden revelations well developed the conflict and the Safe Harbor agreement enabling American public institutions to collect and process Europeans' data was dismissed by the CJEU. Although a newer and more comprehensive system for American companies to prove their consistency with the EU data protection rules was ensured within the Privacy Shield self-certification framework. As we expected, the Privacy Shield agreement was invalidated after the GDPR entered into force (also known as the Schrems II case[137]). Neither the Snowden revelations nor the Schrems cases, however, were not the first and the last data protection scandals caused by the involvement of the American actors.

When famously known Cambridge Analytica scandal was revealed in 2016, people had faced with the undeniable power of algorithmic tools in their very personal choices such as their political opinions. The scandal was referring to Facebook abusing 87 million of its users' data by sharing with a company called Cambridge Analytica which uses a special algorithm to analyze those data to generate personal political content to manipulate people's political opinions serving to Donald Trump's election propaganda. The case is evidential on how far AI technologies could go and affect not just people's personal life, but also to global peace. Further, it proved the importance of the consent mechanism and the existence of consent-aware citizens to make this mechanism work.

Both the EC the MS' DPAs launched investigations not just over Facebook, but the other American tech giants such as Google and Amazon. Although no such crisis has yet occurred between China, who is the world-leading AI investor, and the EU, the difference between the two in terms of the right to data protection is well-known.[138] Before such a scandal occurred, the EU safeguarded with the GDPR.

Besides several other reasons, the basic claim referred in the above-mentioned cases was the data controller's illegal data processing activity, precisely, failure to obtain a valid consent

[134] Giles, 2015, p. 545.

[135] Such as in the case of transferring Passenger Name Records from the EU based companies to the US' related security departments without prior notification or consent of the passengers. Gültekin Varkonyi, 2017c, p. 342.

[136] Tzanau, 2015, p.88. The author describes the collusion between the two continents in terms of privacy undersigned as follows: "security versus privacy; US versus EU antiterrorist legislation; EU versus US legal privacy regime; EP versus Council and Commission; 'commercial processing' of data versus 'law enforcement processing'; and data protection versus data mining".

[137] Judgement of the Court, Facebook Ireland and Schrems, C-311/18, 16 July 2020.

[138] "Do You Care About Chinese Privacy Law? Well, You Should", Li, T., and Zhou Z., [Online], IAPP Privacy Advisor, 8 January 2018, Accessed from: https://iapp.org/news/a/do-you-care-about-chinese-privacy-lawwell-you-should/, Last accessed: 10 October 2019.

of data subjects. This work will put many investigations on the consent obligation of data controllers operating algorithmic calculations in their services, although the consent rule is one of the GDPR's novelties. Before that, we shall specify what personal data is being subjected to this dissertation.

4.3. Definition of personal data in the GDPR

Updated in line with the technological developments, the GDPR significantly broadened the definition of personal data compared to Directive 95/46/EC which did not include the data related to data subjects' online activities (online identifiers, as the Recital 30 of the GDPR refers). Because the technology by the time of drafting the Directive 95/46/EC was quite different, it still could successfully solve the cases in which personal data was related to data subject's online activities. Broadening the meaning of personal data to online personal data is important to ensure legal certainty on the definition of the terms falling under the scope of the EU's data protection law. It is worth noting that, although the updated definition ensures a clearer understanding of what the personal data is, its scope still is being evolved within the CJEU decisions. Recently, CJEU held a decision that the written answers submitted by a candidate taking a professional examination are personal data that were not defined as the same in the Directive 95/46/EC[139]. Besides, questions regarding the scope of personal data affected by personal engagement with technology were referred to the CJEU so often. As a result, the scope of personal data broadened to technical terms such as IP addresses [140]and cookies[141]. AI technologies could expectedly bring a broader understanding of personal data since such data could be automated training data that are born-digital, a new data generated by the algorithm based on the training data, and data about other people collected and processed based on profiling the data subjects.

4.4. Consent rule

Unlikely the Directive 95/46/EC, which did not specify illegality of the opt-out rule, the GDPR strictly binds data controllers to implement opt-in rules for obtaining data subjects' consent. The opt-out rule that is closely related to data controllers bringing pre-ticked boxes before data subjects and tricking them to give their consent, is one of the most significant

[139] Case C-434/16, Peter Nowak v Data Protection Commissioner, [2017], ECLI:EU:C:2017:994

[140] Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, [2016], ECLI:EU:C:2016:779

[141] Case C-673/17, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. [2019], Judgement of the Court, ECLI:EU:C:2019:801.

novelties of the GDPR having its basis in the CJEU case law[142]. Silence or inactivity cannot be considered as the data subject gave consent, therefore such a rule is ensuring the implementation of the opt-in rule. Additionally, Article 7 (4) of the GDPR introduces a data controller to avoid putting consent as a condition of certain service. This means, that the data controller has to keep providing the basic services, therefore data subjects should not be forced to give consent so that they can opt-in based on free will. This rule is connecting the freely-given condition with the validity of the consent. Also, the data controller should inform the data subjects about their identity and the purposes of processing just-in-time when or before the data is being collected[143]. Consent is not valid in such occasions where a clear imbalance of power is visible between data controllers over data subjects. Where the data subject is under pressure in deciding about giving consent or is left out of the basic services offered by the data controller, consent is supposed to be not valid[144]. Emotional pressure could, or at least, should be an example of imbalanced situations.

Article 13 of the GDPR indicates how data controllers shall fulfill their informing duty such as providing information on data controller's identity, contact information, purposes, data transfers to third parties if any, and other similar basic information. A more detailed analysis of the consent rule and the discussions related to the practicability of the consent rule on AI technologies will be presented in the analysis part.

4.5. Data Protection by Design and by Default

Data Protection by Design and by default principles are not entirely new principles, as the inventor of the term Ann Cavoukian[145] listed the privacy by design rules in the 90s, but they entered into the EU legislation only with introduction of the GDPR. Article 25 of the GDPR entitles data controllers to implement "appropriate technical and organizational measures" to ensure full protection of rights of data subjects. Such measures start from data minimization to a variety of Privacy Enhancement Technologies (database privacy, respondent privacy, storage privacy, transparency enhancing techniques, etc.)[146]. The GDPR lays down tangible proactive measures for data controllers to take into account. The EU legislator combines these rules with the DPIA measurements to ensure a complete *data*

[142] Case C-673/17 Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. , Opinion of Advocate General Szpunar delivered on 21 March 2019, ECLI:EU:C:2019:246, para. 72 and 84.

[143] Recital 42 and Recital 61 of the GDPR

[144] EDPB, 2020a, para 24.

[145] Cavoukian, 2010.

[146] Gültekin Várkonyi, 2017b, p.118.

protection first culture[147] by putting the rule in a legally binding document. Even though its efficiency on AI-based technologies is being argued[148] (and it is most probably because of the GDPR's technology neutral nature), it is one of the novelties the GDPR brought on the way to provide a better protection for the EU citizens' right to data protection.

4.6. Data Protection Impact Assessment

Article 35 of the GDPR introduces a new tool for data controllers to self-check and to prove their compliance with the GDPR based on proactive measures. It is a strong guideline to ensure the rights of data subjects based on risk analysis. Although the assessment is to be conducted when the processing activity is "likely to result in a high risk to the rights and freedoms of natural persons", incident 3 of the Article 35[149] gives a clear indication for the data controllers operating algorithmic tools to be entitled with the assessment. Therefore, data controllers using AI technologies (such as social robot providers) most probably have to conduct a DPIA before launching their services, since operating these services would require processing a large scale of personal data.

4.7. National Supervisory Authorities

Articles 51-59 of the GDPR define the rules for establishing an NSA and further explain the competences and powers of the NSA. The main role of the NSA is to ensure consistent application of the GDPR by monitoring the application within the territory of the MS it was established through the competences assigned by the GDPR and the national legislation. The NSAs are established in line with the principle of independence, meaning that they can decide about their constitutional structures, organization, and administrative structures[150]. For example, any MS is free to decide how many NSAs would be established within its territory by guaranteeing a single contact point that would ensure the communication with the other NSAs, the Board and the Commission[151]. This work does not focus on the institutional characteristics of the NSA but highlights some of the relevant competencies are given to the NSAs under the GDPR.

[147] Everson, 2016, p. 30.

[148] van Wysenberg, 2020, p.18.

[149] Article 35 of the GDPR provides the following rule: "A data protection impact assessment shall be required in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which are based on automated processing, including profiling…"

[150] Recital 117 of the GDPR

[151] Recital 119 of the GDPR

First of all, the GDPR ensures corrective, advisory, and investigative powers to the NSAs as Article 58 points. When exercising these powers, NSAs could impose administrative penalties (which could be up to 20 000 000 EUR or up to 4% of the total worldwide annual turnover, according to Article 83) on data controllers and data processors. These amounts are considered higher than the ones imposed under the Directive 95/46/EC.

The NSA safeguards the data subjects' rights towards data controllers with several investigation tools. Citizens could exercise their right to complain about an infringement with the NSA in line with Article 77. Data subjects are given many options (depending on the location of the infringement occurred) when choosing the NSA to complain. Once the NSA received a complaint, data subjects are informed about the progress and outcomes of the complaint within a reasonable period established under the national law.

Only 5 months after the GDPR entered into force, NSAs received thousands of cases. According to the research published by GDPRToday Blog,[152] covering the data from NSAs in Germany, England, Ireland, Italy, Sweden, France, Poland, and Romania, 42.230 complaints were received by these NSAs under the GDPR. Almost 13.000 data breaches were reported and several amounts of fines were imposed. In 2019, the total number of complaints reached about 145.000 by May (without a single significant fine issued to the big-tech companies)[153]. NSAs are the watchdog in the right and consistent enforcement of the GDPR.

Last but not least, the NSAs have the competence to start or take a part in legal proceedings before judicial authorities. The NSAs are now in a stronger position within the country they have jurisdiction, and cooperate with the other NSAs in the EU, together with the EDPB, more than ever before.

5. Technological Developments and New Data Protection Challenges

Even though the GDPR brought a higher level of protection to the rights of the EU citizens and is still the most updated data protection legislation, the fact is that it was drafted in 2016 and entered in to force in 2018. Since then, shortcomings of the GDPR have been heavily discussed in academia from many aspects. Among those, Rossnagel et al. (2018)[154] refer to

[152] GDPR Today, GDPR in Numbers No.1, 25 October 2018, [Online], panoptykon.org ed. Available: https://www.gdprtoday.org/gdpr-in-numbers/ Last visited: 12 December 2019.

[153] The cases handled by the Irish and Luxemburgish DPAs did not result with fine to Facebook, Google, Microsoft, Amazon and PayPal. Access Now, 2019, p.7.

[154] Rossgnagel, 2018, p. 4.

the problems related to practicing the GDPR which gives only abstract and indeterminate provisions. As their work indicates, those provisions could only be concretized by the national DPAs and by the courts[155] which would cause different interpretations. Since 2016, AI technologies have received increased attention from the governments of the EU MS. The GDPR's opening clauses, e.g. regulation of robotics, allow the MS to create their provisions unless it clashes with the GDPR. As this dissertation also will confirm, there is a discrepancy between the sample countries applying the GDPR, also in comparison to the EU, and their ambition and actual regulation on AI. In this work, we argue that the GDPR remains too technologically neutral, meaning that the GDPR prevents legal provisions from excluding technological innovation, including AI technologies, and raises a risk-neutral approach. On the other hand, AI-specific risks to privacy and data protection appear as a result of their design and development processes, together with the real-life implications that will be analyzed in the later chapters. Mainly, the common point of all these three cycles is referring to capturing and extraction of data without the valid consent of the data subjects as well as profiling and affecting them without their knowledge without leaving them an opportunity to intervene[156].

This work focuses on the practical, legal, and technical problems arising from the use of personal social household robots in which the GDPR remains neutral. These problems, as grouped below, will be extensively analyzed in the following section and could be also considered as the hypotheses of this work:

i) *Practical* problems regarding the consent rule:

- People do not read the privacy statements, therefore they usually do not know what they exactly are consenting for.
- Even if they read the privacy statements, they do not understand it completely, but still, give their consent just to use the services offered by the data controllers.
- People may not be fully aware of how AI-based products work, or more specifically, how personal data is being collected and processed in these products. They may not be fully aware of the consequences of having a personal AI-based product at their households.

[155] Ibid.
[156] Leslie, 2020, p.5.

- The companies producing AI-based products or services either may not wish to disclose information regarding the use of personal data within the systems or may not entirely assess the possible implications of AI on right to personal data.

ii) *Technical* aspects of AI technologies raise problems regarding the practicability of the consent rule:

- Principle of purpose limitation which is one of the basic principles of obtaining valid consent is impossible to comply with since AI performs *unpredictable data collection by design*.
- The question of black-box algorithms remains the biggest obstacle before creating explainable AI[157].
- Algorithms are unpredictable by design, which is technically expectable, but not acceptable by law.
- AI technologies, especially social robots, raise a certain level of trust in people (e.g. through their humanoid behaviors) which, in the end, make them think like they could share anything they wish with machines. Social robots can manipulate people's decision making, including sharing their data with the machines referring to the term *uncanny valley.*
- Reinforcement Learning techniques melting the safeguard of the consent mechanism since this technique enables machines to collect and process instant data to make instant decisions.

iii) *Legal* loopholes in the GDPR on the consent rule reinforces the practicability:

- There is no obligation in the GDPR assigned to the data controllers to ensure the understandability of the information they provide to the data subjects, although there are similar rules referred (the rule for "meaningful information" and "intelligible form"[158]).

[157] Adadi and Berrada (2018) put a significant effort on defining the term explainable AI. While they do note that there is no formal definition of the term, they mapped the related terms and also synonyms by conducting a research on the works of the research comunity. As a result, we could understand that explainability does not only refer to explaining the outputs of AI systems but could refer also to the pre-explanations. In terms of fulfilling the consent requirements, the explanation is placed before the algorithmic assessment is made and refers to the transparency and informing obligations. In other cases, explainability refers to the post explanations about the output of the algorithms. We prefer using the terms interchangeably but cautiously, and make the distinction clearly whenever is needed.

[158] Gültekin Várkonyi, 2019, pp. 208-209.

- The right to explanation is an ex-post right and data controllers could choose to fulfill some part of their information obligation about the algorithmic decision-making after the decision is made by the algorithm, not before.
- There is a probability for natural persons to fulfill some of the data controllers' obligations in case they allow their personal household robots to interact with other people.
- Each country subjected to this research (Finland, Italy, the Netherlands, and Hungary) has its "own way" to apply the GDPR in case AI technologies and this vary widely. This may affect the "uniform application" aim of the GDPR if no EU-wide legislation on AI technologies is accepted.

As a result of the questions stated above, this dissertation will further analyze the relevant rules of the GDPR presented in Table 1. The GDPR is an integrated legal document meaning that all the Articles are related and complimentary on each other, however, chosen Articles under the present work are the most-concerned topics specific to the AI and robotics technologies as will be discussed in Part V. To make the connection between the chosen Articles and the concerns noted in Part V, we first shall define the technology dealt with in this work.

Principles	Rights of Data Subject	Data Controller's Obligations	National Supervisory Authorities
Art. 5 (1) (b) Purpose Limitation Art. 6 (a) Lawfulness of processing- Consent rule Art. 7 Conditions for consent	Art. 22 Automated individual decision-making, including profiling Art. 12 Transparent information, communication and modalities for the exercise of the rights of the data subject Art. 13 Information to be provided where personal data are collected from the data subject Art. 22 Automated individual decision-making, including profiling	Art. 24 Responsibility of the controller Art. 26 Joint controllers Art. 25 Data protection by design and by default Art. 35 (3) (a) Data protection impact assessment	Art. 57 Tasks Art. 58 Powers

Table 1. Relevant GDPR Articles Subjected to Analysis.

III. Definition of Artificial Intelligence and Personal Social Robots

1. Definition of Artificial Intelligence and the Related Terms

The term AI was first used to indicate the "creation of a humanoid machine"[159] which could be called also as the "machina sapiens"[160]. Such a machine could be further defined by referring to its functions which bringing them closer to be human-alike. For example, Britannica's definition draws the attentions to AI's "ability to perform tasks that are executed by intelligent beings like humans, in a digital or physical form like robots, via computers"[161]. Even this basic encyclopedic definition shows a degree of a relationship between AI and humanoid robots. Further, Intel's AI definition, similar to the Britannica definition, indicates that "AI is a simple vision where computers become indistinguishable between humans"[162]. Until now, presented definitions focused on AI's intelligent and autonomous capabilities which are compatible with human abilities, but Floridi and Sanders further added interactivity and self-learning capabilities of AI to those definitions [163]. Moreover, Kirchberger[164] explains what an AI is based on four specifications, which the first three are, that acting humanly, thinking humanly, and thinking rationally. The last specification refers to the AI's ability to act autonomously to perceive its environment, the ability to adapt to changes, create goals, and act rationally to achieve the best outcome of its actions.

Specific to the robotics, Murphy [165] identifies seven subdivisions for AI robots each highlighting a broad scientific field of modern robotics. The first subdivision refers to knowledge representation enabling a robot to find out how to reflect its actions in the real world. Natural language and natural language processing stand for the use of and understanding of the natural human language. Further, planning and problem solving (motion planning or problem-solving); inference (to prevent robot to reach incomplete or inaccurate data); search; and vision (triggering the robot's actions) form the other subcomponents of a robot. Finally, learning (from the experience) is a unique behavior of robots enhanced with ML techniques. One may easily realize that the subdivisions are inspired from the human-specific actions or behaviors while some of them could be applied

[159] Li and Jiang, 2017, p.381.
[160] Hallevy, 2010, p. 5.
[161] "Artificial intelligence", B.J. Copeland, [Online], Britannica. Accessed from: https://www.britannica.com/technology/artificial-intelligence Last accessed: 6 October 2018.
[162] This definition belongs to Pradeep Dubey, academician and Intel Fellow at Intel Labs. Accessed from: https://newsroom.intel.com/news/many-ways-define-artificial-intelligence/ Last accessed: 6 October 2019.
[163] Floridi and Sanders, 2004, p. 7-8.
[164] Kirchberger, 2017, p. 195.
[165] Murphy, 2001, p.248.

with hardware support, what makes AI special is the ML letting the robots to process data and to use that data meaningfully. ML is an integrated part of AI systems helping to reach all these goals starting with gathering the necessary data (either past training data or acquiring new data through self-training)[166.]

1.1. Machine Learning

If machines are reacting only to known situations and always in certain ways, they cannot adjust themselves to the changing environments. Adaptation, as referred previously, is an element of intelligent systems. Only a learning machine could have an adaptation ability which is the basic rule of autonomous robots[167]. Learning, or Machine Learning, is "one particular form of AI, which gives computers the ability to learn from and improve with experience, without being explicitly programmed", clearly, without an impactful human intervention leaving the robot itself to learn[168]. Through ML, the algorithm learns to create own decision-making rules unlikely to the classic programs where the rules are pre-defined[169].

ML methods have a crucial impact on collection and processing (personal) data. Consequences of applying a certain method differ if a machine was given a data pack to learn (such is the case for Narrow AI or Supervised Learning) or it captures and evaluates data on its own (e.g. Reinforcement Deep Learning). In Supervised Learning, for example, classifying credit applicants in a low risk or high-risk credit group is possible by analyzing applicants' data based on a model in which the rules were already defined[170]. The model might be created based on the individuals' data such as the salary, debts, profession, performance of covering the debts, and so forth, or based on a group of chosen criteria. The algorithm marks the variables of each group with the known rules and generates a score with a probability placing the polled case in a high-risk group or a low-risk group. Each credit application might be decided based on the applicant's (who could also be named as a data subject) belonging to these groups affecting the final decision of the creditor. Such

[166] Taddy, 2019, p.63.

[167] We strictly leave out philosophical discussions related to autonomy, and we adopt the perception of robots' autonomy which is possible with their ability to make autonomous decisions through their data collection and processing capability together with learning capability.

[168] Kirchberger, 2017, p. 197.

[169] Sandvig et al., 2016, p. 4978.

[170] Alpaydın, 2016, p.46.

automated decision-making procedures together with their outcomes are definitely based on personal data and the GDPR is fully applicable to such cases.

A robot can learn without such a supervision meaning that no output is predefined[171] which refers to the technique called Unsupervised Learning. Aim of this technique is to make algorithms to identify the patterns in a large dataset to, for example, the group of people showing similar behaviors without predefining the groups[172]. Each cluster may identify consumers' personalities such as in the following example; X user is likely to prefer newspapers with political content, Y user may prefer non-alcoholic drinks, Z user may prefer slow music. The machine could make such estimations from the raw data collected directly from the environment and label them itself. More clusters the algorithms create, more about they could get know about a person. There are several ML techniques a social robot to be deployed for learning and serving humans in a personalized way.

A typical ML lifecycle consists of data collection, data preparation, model development, model evaluation, model post-processing, and model deployment[173]. Clearly, data collection is the first step influencing the future of the other steps. Data collection, as the most time-consuming stage of ML, is the basis of the ML, and apparently small datasets may cause lower accuracy although there is no specific number indicating whether the data set and observations are enough to train it, but still, amount of data should be big enough for the developers to test the variables accurately and precisely[174]. In an unsupervised learning technique, as well as in the RL, these variables are set following the machine's needs, therefore the data needed to further train the system is subjected to the algorithm's evaluation, with a developer's small interference. To our view, this is one of the successes of the neural network models which are complex but more accurate than the simple models[175]. Simple models are also easier to explain in comparison to the complex ones as such the Deep Learning techniques produce.

1.2. Deep Learning and Neural Networks

Deep Learning and Deep Neural Networks (simulating human brain into machine language), have been heavily used for improving current robot capabilities which are yet improved a

[171] Ibid., p.111.

[172] Rhoen and Feng, 2018, p.143.

[173] Suresh and Guttag, 2019, n.p.

[174] Lehr and Ohm, p. 679.

[175] Ibid., p.693.

limited level. If this method is used, AI systems evaluate each data differently in every layer. Layers have consisted of nodes that functionality derives from non-linear activations passing to a linear combination of inputs[176]. These are modular layers that are combinable with one layer optimized for a type of data to another type of data[177]. In this case, every layer is connected to one or more layers, according to the data used. If the data is important, the AI system remembers and uses it more often stimulating the connection between the layers stronger. If each layer is structured according to their different roles by the algorithm, it might be difficult to find out what data has been used for which role. The machine analyzes a question abstractly and answers to it again in an abstract way[178] meaning that finding out an explanation for the outputs may not always be possible (e.g., as the black-box algorithms refer). This explicability question will be analyzed in further chapters in the frame of consent and purpose limitation. If the decision carries a certain degree of autonomy, then the risk of rendering the AI's action becomes unforeseeable and unexplainable at some point[179]. Once a social robot makes a decision (generates an output) question of explicability may even be more difficult if the machine learns directly from human interactions.

1.3. Reinforcement Learning

Reinforcement Learning or Deep Reinforcement Learning is a technique providing active learning to machines by rewarding and punishing them, similar to Pavlov's classical conditioning. It is an emergent DL technique gaining more attention in academia since it aims to raise the abilities of AI systems to learn from raw data that could produce full autonomy for robots[180]. Robot gains the reward at the end of HRI (might be receiving its reward directly from the user/data subject), and learn faster and better if the reward is bigger. This behavior is named reward-driven behavior[181]. More importantly, it becomes better personalized after each reward, so it could express concrete personalized behaviors by time. This technique is one of the best ML choices for robots that could learn from experience and interaction in the real world[182] because only then someone would think of gaining a social robot at home assisting in the daily life routines. RL is a method used for predicting not

[176] Taddy, 2019, p.8.
[177] Ibid., p.9.
[178] Alpaydin, p. 93.
[179] EP, 2017, para. AI.
[180] Arulkumaran, et. al., p.1.
[181] Ibid., p. 2.
[182] Haarnoja et. al., 2019, p.11.

human behaviors at first sight, but developing a strategy to predict human's next action, by learning[183] and robot's personality plays a crucial role in this sense.

1.4. Personalization through Reinforcement Learning

The idea of personalization of robots is vested in the Google patent[184] creating social robots that could adapt and develop a personality with the help of RL techniques. Theoretically, the user gives some feedbacks for the actions of the robot or feeds the input data to the robot to make it understand a statement. For example, if the user pats the robot's head, it can understand the user's emotional status and respond accordingly. If a user gives a negative reaction to the robot's action, then it could understand that the user is not pleased with its action. As it is clear, this procedure is possible to follow through HRI or CHI, or with the approach known as Use Centered Intelligent Environments Development Process where the team of the system development consults with the end-users at every step of development until and after production[185]. Either of the approaches might be adopted since personal services mean more personal data and people will not fear to share their data with robots to gain personal services[186].

Researches in the field of AI and RL focus mostly on social robots since social robots are planned to be introduced in person-centric services, such as health-care and education. For example, Leyzberg, Ramachandran, and Scassellati[187] proved that social robots assisting children to learn a second language with personalized content bring more success than the non-personalized ones. Children helped the algorithm to dynamically set its teaching method according to their feedback and optimize both the positive feedbacks delivered by the children, therefore maximize children's learning skills. There is no doubt, that such a social robot could help children to learn faster and more efficiently in comparison to a robot deployed with pre-determined content. Another research was conducted to find out what topics should the students make practices of to learn more, and a robot that could learn from individual students' skills (followed by the other inputs such as students' non-verbal behaviors) were used for an experiment. This work also proved that a social robot deployed with an RL technique helped students to fulfill their knowledge gap under their school

[183] Kar han tan, 2018, p.9.
[184] Google, Methods and systems for robot personality development, U.S. Patent 8996 429 B1 31 March 2015.
[185] Augusto et. al., 2018, p.116 and p. 128. This work shows how user-centric system design could and should be, present the fact that without entering into the private life and sphere of the users, there cannot be an almost perfect intelligent product. The work has pioneered such an issue under the ethical framework statements.
[186] Coopamootoo, and Groß, 2017, p. 40.
[187] Leyzberg., Ramachandran, and Scassellati, 2018, p.11.

curriculum[188]. Besides the academy, the industry invests on RL based systems such as the case with Google's DeepMind[189], and IBM's Watson[190], or Facebook[191] and Amazon[192].

1.5. General AI

General AI, Artificial General AI, Strong AI, or Superintelligent, refer to AI that could reach or surpass human-level intelligence. Although there are many back and forth around the technical discussions, some researchers predict that by 2050[193] there will be a representation of General AI in our lives. Boström foresees General AI equipped with several other techniques such as cognitive computing to execute very general cognitive tasks working better than current human intelligence to happen soon after the human-level machine intelligence is developed[194]. If they could represent "compositional, hierarchical, and causal representations" in their learning path[195] and "could successfully break the problems down in components that ML could solve"[196], then there is no obstacle before AI to surpass human intelligence. Our position in this discussion is that regardless of the conscious mind or being superintelligent, AI still could raise risks over people's privacy, so we do not consider to discuss this argument within this work. Actually, with such machines around, there will be no meaning of privacy in traditional terms, but we leave this topic out of this work.

Superintelligents are unlikely to be a form of robots, but they also could be transformed-human like a cyborg. Whole brain emulation or mind uploading researches[197] are being conducted to find out how the human brain could be simulated in computers and pave the way for Singularity. In our work, we would like to once again stress that we focus mostly on robots, not on cyber organisms. But the reason why we include this statement is related to

[188] Ibid., p.13.

[189] "Deep Reinforcement Learning", David Silver, [Online], Deep Mind Blog, 17 June 2016 Accessed from: https://deepmind.com/blog/article/deep-reinforcement-learning. Last accessed: 7 October 2019

[190] "Train a software agent to behave rationally with reinforcement learning", M.Tim Jones, [Online], IBM, 11 October 2017 Accessed from: https://developer.ibm.com/articles/cc-reinforcement-learning-train-software-agent/ Last accessed: 7 October 2019

[191] "Advancing AI by teaching robots to learn" Franziska Meier, Akshara Rai, Roberto Calandra, [Online], Facebook AI Blog, 16 May 2019. Accessed from: https://ai.facebook.com/blog/advancing-ai-by-teaching-robots-to-learn/ Last accessed: 7 October 2019

[192] "Use Reinforcement Learning with Amazon SageMaker", [Online], AWS, Accessed from: https://docs.aws.amazon.com/sagemaker/latest/dg/reinforcement-learning.html Last accessed: 7 October 2019

[193] Müller and Bostrom, 2016, p. 560.

[194] Bostrom, 2017, p.20 and p.36.

[195] Lake et. al., 2017, p.30.

[196] Taddy, 2019, p.64.

[197] Alcor Foundation has more than 100 "patients" cryonized. See: https://alcor.org/profiles/index.html Last accessed: 2 January 2020.

the EU's confusing statements regarding robots. In some of its official documents, the EU puts stress on assigning an electronic personality to robots in which the term was noted by Karnow[198], but then later claims that there would never be a Superintelligent in the world[199], therefore such discussions should be left aside. In another document, the EU states the possibility for Superintelligents to become alive and offers a safeguard (human in command)[200] against such robots. The present work also emphasizes the importance of putting humans in control, confirming the human-in-the-loop philosophy.

2. The European Union's Artificial Intelligence Definition

"Artificial intelligence is not science fiction; it is already part of our everyday lives, from using a virtual personal assistant to organize our day, to having our phones suggest songs we might like"[201]

As highlighted in the definitions section, the EU has long been lacked a single AI definition like the industry and academia. The earliest efforts were given by the EU institutions to make an AI definition goes back only to the year 2018. Several EC Communications drew a very short and general AI definition that made it almost impossible to differ AI from the other general technologies in basic terms[202]. For instance, those definitions excluded the core abilities of AI that are data processing, learning, and acting, and focused only on the intelligence and autonomy aspects in a general sense. Only after the formation of HLEGAI in April 2019, the EU reached a formal AI definition pointing almost the entire specifications of AI technology, as follows[203]:

> "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected

[198] Karnow, 1994, p.4.
Karnow's concept for electronic personality (or the "epers", as he calls) consists of several elements such as identity (owing money and bank accounts together with being able to apply for bank credits), ability to complete its task without intervention, and communicate with other electronic persons. It should be noted that Karnow's inspiration based on the legal construction of public and private companies that are not physically presented, but have an identity (dominantly affected from financial presence) as the human has. He further conceptualizes the identity of the electronic persons specific to hold privacy rights, free from discrimination, and free speech. This framework also stresses that electronic persons are different than tangible properties like cars, and should be created to protect humans not replace them.

[199] Bentley et. al., 2018, p.22.

[200] European Economic and Social Committee, 2017, point 3.42 and 5.2

[201] Opening speech of Commissioner Mariya Gabriel at AI Forum in Helsinki, 09 October 2018.

[202] EC, 2018c, p. 1 "Artificial Intelligence refers to systems that display intelligent behavior by analyzing their environment and taking action — with some degree of autonomy — to achieve specific goals".

[203] HLEGAI, 2019a.

> structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behavior by analyzing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors, and actuators, as well as the integration of all other techniques into cyber-physical systems)"

It is important to note that the above definition was given almost three years after the GDPR was enacted and a year after it entered into force. This certainly points that, the EU lawmakers did not have a chance to entirely evaluate and insert possible AI-related data breaches in the legal text, e.g., based on a relationship with personal data and ML techniques[204] by the time of drafting. This would be important to take into account since these aspects of the AI are closely related to collection and processing (big amount) of data, its capability to generate knowledge[205]. Even though the GDPR is technology-neutral legislation, questions regarding these very specific aspects could have been answered by embedding them in the general rules and principles, or more interpretation and guidelines could have been delivered by the time.

As the definition proves, and as we will reinforce in Section IV, there is a close relationship between AI and robotics, especially, between the service robots, according to the EU. AI could be able to perform useful tasks in an embodied form more than it could as a software[206]. Further will be presented below, AI in the robotic body could serve to lift the quality of people's private life by performing the tasks belong to and within a household, moving freely in, and collecting an enormous amount of data by the help of its physical presence. Before discussing all the possible risks towards an individual's data protection

[204] Matthias, 2004, p.177.
"That would be particularly important to discuss the liability issues. The core of the ML is that the rules by which they (machines) act are not fixed during the production process, but can be changed during the operation of the machine, by the machine itself."
Matthias also presents short scenarios to illustrate his position.

[205] Microsoft, 2018, p. 29.

[206] Nath and Vineet, 2017, n.p.

rights deriving from personal use of robots, more specification will be made about what kind of robot does this work refer to.

3. Definition of Robot

Different perceptions and concepts about the use of robots in different fields make it difficult to put a general definition of robots. For example, the International Standard Organization defines a robot as "an actuated mechanism programmable in two or more axes with a degree of autonomy**,** moving within its environment, to perform intended tasks[207]. This technical definition reflects only the mechanical component of a robot, leaving aside the possible deployment of it with AI. On the other hand, and way much apart from a technical definition, the social definition of robots has emerged (public deception) caused by Sci-Fi literature. Robots have long been illustrated as they are human's enemy, not contributing much to reach a scientific definition. Several efforts in academia helped to fix this situation. For instance, Richards and Smart analyzed how robots are perceived in Sci-Fi films, which affects people's perception of the robot, in comparison with how they are in real life. They proposed the following definition by stressing what do people think based on Sci-Fi literature: "A robot is a constructed system that displays both physical and mental agency, but is not alive in the biological sense"[208]; at least, this definition has a more neutral meaning. However, even if they are not alive, they are present in real life with their senses (e.g. via sensors), thoughts (e.g. ML), and actions (execution of a task in the real world) to tackle the dynamic real-world situations. The HLEGAI's efforts resulted in a robot definition where robot's functionalities such as "perception, reasoning, action, learning, as well as interaction capabilities with other systems" are highlighted and counted as an integrated part of robotic systems[209]. At this point, one could once again easily see the connection between robots and AI since they are both able to sense, think, and act, as we mentioned during the AI definitions section. However, robots have more opportunities of collecting data since they are equipped with hardware enabling them to interact with the real world closely. Sensors of a robot enable them to access many different types of data, let it be equipped with RFID systems, gyroscope, accelerometer, GPS, wireless sensors, infrared sensors, optical sensors, and biosensors[210] besides cameras, microphones, and variety of actuators. While the definitions of the robot are quite comprehensive and generally made, the types of the robot should be

[207] ISO 8373:2012(en) Robots and robotic devices - Vocabulary, para 2.6.

[208] Richards and Smart, 2015, p.6.

[209] HLEGAI, 2019a, p.4.

[210] Google, Methods and systems for robot personality development, p.7.

mentioned to make the last distinction between the robot subjected to this work and the others.

3.1. Service Robots

Unlikely the definition of robots, typology of robots is categorized in a more unified way both in academia[211] and industry. This is, indeed, due to the distinctive functions of each type of robot that were classified by the IFR under two based on their functionality; industrial robots and service robots. Industrial robots are being used mostly for the production of a good, such as in the automotive industry, electronics, metal and machinery, rubber and plastics, food and beverage industry[212]. Service robots, on the other hand, serves to personal goals such as household robots (e.g. cleaning, cooking) or for professional use such as medical care and entertainment (toys and hobby systems). A service robot's functionality surely could overlap between the personal and professional goals; e.g. a robot could entertain also individuals that does not require professional use. Focusing on a specific type of robot helps us more to define what a robot is, but we avoid making a general definition for robots since we focus only on social robots which are one of the subtypes of a service robot.

Determining a specific type of robot was one of the initial phases during the preparation of the present work. While the term service robots remain too general for research like ours, we were looking for a specific term highlighting the personal use of service robots. With this aim, we looked for several resources to conceptualize the personal use of service robots. Available ISO's vocabulary considers three terms close to fulfilling this aim. First, the term service robot[213] was found that is referring to such robots that are performing useful tasks for humans and strictly excluding industrial robots. This approach represents service robots serving food, cleaning, or providing health-care services to people[214]. Then personal service robots, on the other hand, functions same as the service robots, but only for personal use, excluding commercial activities. Finally, we found the term collaborative robots in the ISO's

[211] Fosch-Villaronga comprehensively analyzed the legal and ethical aspects of personal care robots. Although he strictly stated that not only social robots but all the personal care robots, our intention in this work is to pick social robots as a case for data protection specific.
Fosch-Villaronga, 2017.

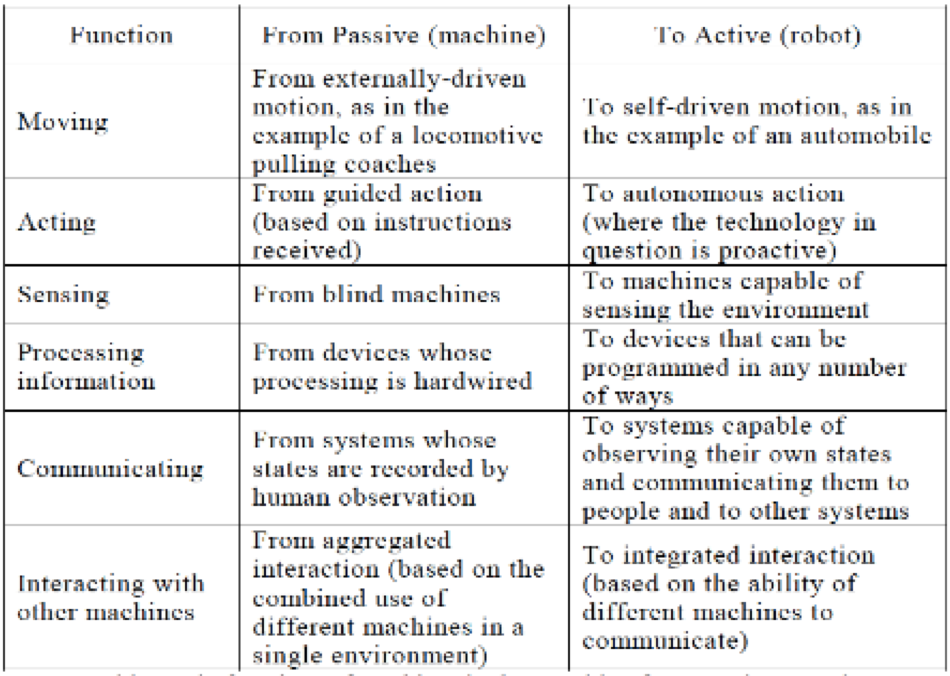
[212] International Federation of Robotics, "Executive Summary World Robotics 2017 Industrial Robots" [Online]. Available at: https://ifr.org/downloads/press/Executive_Summary_WR_2017_Industrial_Robots.pdf Last accessed 8 November 2019.

[213] ISO 8373: 2012, paragraph 2.10

[214] Ibid., paragraph 2.11

vocabulary, referring to a type of robot which can enter into an interaction with a human[215]. All these definitions point out a personal use of non-commercial robots which can show some degree of interaction with its user. The term social robot involves all these aspects, as will be soon demostrated.

The final approach, which is also the final reason why this work focuses on social robots, is related to robots' definition from their capabilities point of view, based on Laukyte's analysis. In her research, Laukyte focused on the basic functions of robots (moving, acting, sensing, processing information and data, communicating, and interacting with other machines) switching them from being passive machines to being active robots. The capabilities approach originally defined around the ten human capabilities to be respected and protected by states as Nussbaum[216] discovered and extended on animals[217], while Laukyte extended Nussbaum's work on robots[218].



Function	From Passive (machine)	To Active (robot)
Moving	From externally-driven motion, as in the example of a locomotive pulling coaches	To self-driven motion, as in the example of an automobile
Acting	From guided action (based on instructions received)	To autonomous action (where the technology in question is proactive)
Sensing	From blind machines	To machines capable of sensing the environment
Processing information	From devices whose processing is hardwired	To devices that can be programmed in any number of ways
Communicating	From systems whose states are recorded by human observation	To systems capable of observing their own states and communicating them to people and to other systems
Interacting with other machines	From aggregated interaction (based on the combined use of different machines in a single environment)	To integrated interaction (based on the ability of different machines to communicate)

Figure 3. Functional approach to the machines inspired by human capabilities.
Source: Laukyte, 2015, p.6.

This dissertation also adopts a functional approach for social robots since those functions assigned them a capability to self-drive and to present autonomous actions, to sense and understand their environment, to process information, to enter into communication and interaction with machines and humans around. These capabilities, to our view, are the main

[215] Ibid., paragraph 2.26
[216] Nussbaum, 2011.
[217] Nussbaum, 2004.
[218] Laukyte, 2015, p.6.

differences between the embodied and disembodied AI. An AI software would have restricted functions without those capabilities (e.g. moving, sensing). On the other hand, these functions enable robots to collect more data about things and humans around them. Data is the main input of AI, and robots without AI would be lack all those previously mentioned capabilities.

3.2. Robots with Artificial Intelligence

As indicated before, this work presents a clear position on the embodied AI. By being in the real world, AI would be more intelligent and will be perceived as more real[219]. In this work, we exclude the researches going on cyborgs and mind uploading, therefore we focus only on machines equipped with AI. Embodiment is a factor affecting the legal regulation of AI serving humans in private spaces. For social robots, one of the elements for AI to contact humans is a physical appearance, while the other one is its capability to analyze and reflect their social behaviors. Embodiment is also the main factor that differentiates chatbots, social bots, or avatars from social robots[220]. If a disembodied AI is considered for legal research, the term social bot should have been used instead of the term social robot[221]. In this case, a social bot's presence is virtual, not physical, although the software anyway needs to be deployed in a physical device like a computer or a mobile phone. Unlike virtual agents, they are physically present in the real world, and with this presence, they raise privacy considerations more than the virtual agents. Indeed, a simple house cleaner robot cannot be a discussion[222] of legal literature from the data protection point of view. For this reason, this work focuses on social robots as a case analysis.

3.3. Personal Household Social Robots

Since the Industrial Revolution, humans and robots interact in some and many ways, e.g. via physical commands, and at some level e.g. pre-defined static tasks. In the present time, human interacts with the machine not only in a physical way but in other ways such as verbal, visual, and emotional. As a result of HRI in a social way, a specific type of service robot,

[219] Leroux et al., 2018, p. 60.

[220] Korn, Bieber, and Fron, 2018, p.188.

[221] Alves de Lima, Sarge and Berente, 2017, p. 1.

[222] Actually, it was a discussion once, see whether Roomba's iRobot could model the houses it cleans which may be a threat to privacy. See: "Roomba vacuum maker iRobot betting big on the 'smart' home", Jan Wolfe, n.d. Accessed from: https://www.reuters.com/article/us-irobot-strategy-idUSKBN1A91A5?il=0 Last accessed: 15 November 2019.

the so-called social robot comes along with its abilities to express and perceive emotions, communicate with humans, use human-like reactions, in short, act like a human.

The term social robot, which is the more generally known term, is not a fully accepted expression, and the reason behind this statement is not because of a lack of common definition (as the case was for the definition of AI and robot), but practical and different use of terms by the academia. There are different terms found in the literature used for a social robot[223], for example, societal robot[224], sociable robot[225], and socially interactive robots[226]. Fosch-Villaronga refers to social robots as Companion Robots, Carebots, or Care Robotsin his work in which he comprehensively analyzes the term and prefers to use the term socially assistive robots[227]. This term is different from mobile servants and physically assistive robots that easily could be confused with social robots. According to the author, socially assistive robots are different from the other two types, initially because they socially interact with a human without physical contact. To illustrate this, he benefits from a scenario of a social robot inspired by the Mihajlo Pupin robot (which is now replaced with Nao robot) assisting people with ADL[228] that is accepted as a social robot in the literature. We prefer to use the term social robot to ensure uniformity in this work. We also would like to once again note here, that, whenever we use the term robot, we mean a Robot with AI, not an industrial robot or a simple home robot.

Social robots are certainly not physical assistant robots who do not strictly interact with a human and they also are not personal care robots in a general sense. They could serve humans in any field, not necessarily only in the health-care domain as it is mainly the case for physical assistant robots. As Fosch-Villaronga analyzes personal assistant robots comprehensively[229], social robots could be categorized as mobile servant robots since they are (also) capable of interacting with people socially, moving freely, and they are ready to

[223] Hegel, et. al., 2009, p. 169.

[224] Duffy, et. al., 1999, n.p.
The aim of the authors actually is to introduce the term social robot, however, the authors make a difference between a social robot and a societal robot which is a robot "introduced into society with degrees of required functionality to act as aides to people." The authors did not cite any resource usingthe term societal robot, but we found some resources using the term societal robot. For example, one of the areas of specialization of Professor Wagatsuma is Societal Robot. See: https://researchmap.jp/wagaKBR_/?lang=english Last accessed: 10 January 2020.
Professor Balch also used the term in Balch, T. (2005) 'Communication, Diversity and Learning: Cornerstones of Swarm Behavior BT - Swarm Robotics', in Şahin, E. and Spears, W. M. (eds). Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 21–30.

[225] Breazeal, 2002.

[226] Fong, Nourbakhsh, Dautenhahn, 2003, p. 145.

[227] Fosch-Villaronga, 2017, p. 206.

[228] Project official website: http://www.pupin.rs/RnDProfile/ Last accessed 19 February 2019

[229] Fosch-Villaronga, 2017, p. 52.

serve humanity. Mobile Servant Robot is defined[230] by the ISO as "it is capable of traveling to perform serving tasks in interaction with humans, such as handling objects or exchanging information". Remembering the definition for the social robot above, one could easily realize that this definition is far from stressing the social, emotional, and communicative aspects of social robots. Social robots should be able to demonstrate a range of human capacities such as emotions. They should be able to enter into verbal capabilities, understand humans, and form social relationships with them and should be able to learn all these capabilities themselves.[231]

Although the term social robot has not always been referred in the same way in academia, the definition of the term could be observed in a more unified way. Breazeal's and Fong et. al.'s analyses make a clear definition of a social robot in this sense, that is a robot capable of understanding human social behaviors, interact them in a socially meaningful way through its physical or robot-personal capabilities (such as oral communication, emotions, gestures), adapt itself according to a dynamic social environment, and simulate human behaviors. Fong et al. assigned the following human social characteristics that social robots also carry: "expression and/or perception of emotions; communication with high-level dialogue; learning/recognizing models of other agents; establishing/maintaining social relationships; using natural cues; exhibit distinctive personality and character; may learn/develop social competencies", briefly, most of the social aspects of homo-sapiens. All these capabilities and definitions stress the distinctive features of social robots than other robots.

Such definitions and characteristics, on the other hand, may not meet the practical understanding of a social robot from society's point of view, because there could already be a perception about a social robot in people's minds. Whenever it has been said a word of social robot there may appear several different images in one's mind, mostly and again, as a result of the fallacious image drawn by Sci-Fi literature. If social robots are not dangerous by luck, since this is the case presented in most of the Sci-Fi films, then they are presented as friendly beings, or even more than a friend, as a partner for humans which leads to another deceptive perception. This is particularly dangerous because without knowing what people will exactly face, it is hard to predict the consequences of accepting them into their lives, even if it is positive or negative. However, the situation could be turned into an advantageous

[230] ISO 13482:2014 Robots and robotic devices — Safety requirements for personal care robots.

[231] Moodley, T. (2017). "Understanding social robotics", [Online]. Robohub, 24 January 2017. Accessed from: http://robohub.org/understandingsocial-robotics/ Last accessed: 10 January 2020.

one, as we could find out the dominant features of social robots to illustrate them correctly. Anyway, apart from those extreme examples, some parts of what the Sci-Fi literature showed becomes slowly real today. Social robots that are being developed in the labs are the strongest evidence of such a statement, helping to fix this wrong perception.

All in all, a social robot might be illustrated as a humanoid entity that is as intelligent as human (or sometimes even more intelligent than human) and is in constant interaction with its environment to assist humans in different aspects of their life.

Social Robots may be one of the most emerging areas calling for regulation since they heavily aim at personal use where humans and robots interact not only through simple commands or physical interactions but also through emotional statements. What today humans wish the social robots to be like in the future, e.g. whether they should be designed as emotion-sensing with ethical reasoning or not, will shed light on future realities.

Thanks to the technologies, such as social media tools, where humans create, express or continue their social life and emotions in a virtual form unlikely to the traditional face-to-face physical form, today it is possible to enter into a social relationship with machines like mobile phone or computers. There are already scientific works proving the possibility to develop a system with the help of Convolutional Neural Networks that process and convert raw audio and visual data into a meaningful but spontaneous emotional prediction[232]. RL aims to deploy robots to learn from humans directly and through interaction which makes each robot having a different character just as their human companies have. Whichever technique is being used, social robots will be developed to deliver personalized services which would require the deployment of personal data processing ability in the robot (Natural Language Processing, Image Processing, interactive learning, etc.). That personal data might be either before or after encoded to the robot meets humans. This helps people to accept social robots into their life easier and make them part of their life as well as their private life. We will discuss these themes in the frame of data protection law in the later sections.

[232] Tzirakis, et. al., 2017, p. 1305.

3.4. Social Robots in Everyday Life

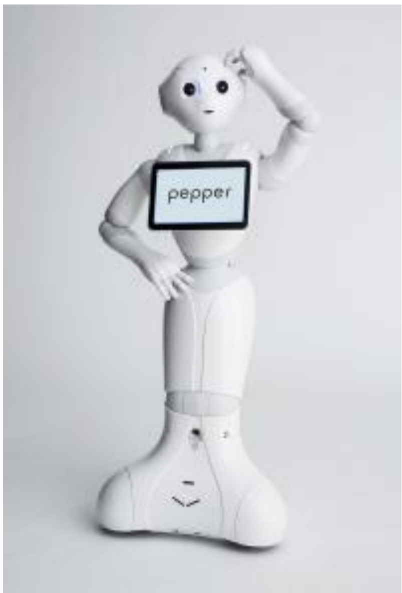


Figure 4. A Social Robot I
Source: Softbank Robotics official website

Based on the definitions above, several service robots could be found even in today's robotic markets. They are already available to engage with people's professional and personal life. Since the first humanoid robot, Eric, was introduced in 1928[233] followed by another humanoid from 1940[234], much has been developed with current social robotic applications that are available in personal use. They would give an overview of how far the technology is today and how far it could continue to grow, both highlighting the emergence of the topic at hand. Putting a limit on types of social robots in practice is a difficult task. For example, self-driving cars are also considered to be a social robot, however, their initial aim is not to interact with people socially. In this work, only the robots which can socially interact with people and enter into their homes are subjected to analysis and this is the main reason why we refer them as Household Social Robots (HSR). Although they could have distinctive tasks such as education, entertainment, healthcare, and home security, we will focus on social robots created for multiple purposes for personal use[235].

The history of social robots goes back to the late '40s[236], in line with the invention time of humanoid robots, but affordable hardware combined with continuously developing software engineering abilities makes it possible to live with us today. A French company, Aldebaran, designed a robot named Pepper (deployed with narrow AI) to live with humans who "can

[233] Eric Robot, 1928. Available at: http://www.richardsrobots.com/eric-robot.html Last accessed: 10 June 2020.

[234] Marsh, E. "Elektro the Moto-Man Had the Biggest Brain at the 1939 World's Fair", IEEE Spectrum, 28 September 2018. Available at: https://spectrum.ieee.org/tech-history/dawn-of-electronics/elektro-the-motoman-had-the-biggest-brain-at-the-1939-worlds-fair Last accessed: 10 June 2020.
Between 1970 and 1984, Waseda University projected two humanoid robots called WABOT. Source: http://www.humanoid.waseda.ac.jp/booklet/kato_2.html Last accessed: 10 June 2020. There are obviously more humanoid and social robot examples, but these examples are chosen to point the fact that chronologically there have always been humanoid robots in the history.

[235] Fosch-Villaronga and Albo-Canals, 2019, p.78, defines three types of social robots with therapy purposes: a robot as a companion, a playful tool, and a coach. We believe that there will not be such a clear distinction among social robots aiming to increase the quality of people's lives at their households and the industry tendencies are more favorable investing in multi-purpose robots.

[236] Fong, Nourbakhsh and Dautenhahn, p. 143.

tell when humans are happy, sad, or angry just by looking at their faces, and can cheer them up". Aldebaran sold some 7000 of them for a price of $2000 each[237] in 2016. A US-based Avatarmind's robot iPal offers friendship to children, plays with them, naturally talks to them, and learns about them. iPal even assists them in learning activities by interacting with them[238]. Besides coaching humans to learn or solve problems, these robots are also aware of emotional cues and can manipulate humans via emotional statements and interactions. Even more, they share people's most private moments while they assist them to have a better sexual life[239]. Robots presented in the TV shows, like the robot *lady* Sophia (who was awarded citizenship by the Saudi Government and became an Innovation Ambassador for the United Nations Development Programme), are designed for entertainment. Sophia's kind of robots may never aim to make people's life better, just to entertain them.

Having a social robot with advanced AI capabilities at home may not be present time's reality, yet, since creating such robots requires a lot of investments (on hardware and software, maintenance, development, etc.) and acceptance by the public. However, CloudMinds robotics promises to launch social robots (humanoid robots, with their words) with affordable prices for the household by 2050, therefore launched the XR-1 social robot project. This robot could interact with people, understand the interaction and its main tasks. Such tasks might be of bringing coffee and guiding a thread into the small hole of a needle without a mistake[240]. It is supported by 3D object recognition, NLP, image processing and other technologies that operate all in its cloud storage.

Figure 5. A Social Robot II
"*The robot, Sophia, personifies our dreams for the future of AI*"
Source: Hanson Robotics official website

[237] Winfrey, G., (2016) "Meet the Robot Coming to Businesses and Homes This Year", [Online]. Inc.Accessed from: https://www.inc.com/graham-winfrey/introducing-pepper-the-friendly-humanoid-robot.html. Last accessed 26 October 2019.

[238] KPMG, (2016) "Social Robots". [Online].
Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/social-robots.pdf. Last accessed 12 December 2017.

[239] Realbotix is offering customizable sex robots, see: https://realbotix.com
Nowadays, the company is planning to launch a Siri-like personal assistant specialized in phone-sex. Last accessed: 20 April 2019.

[240] "CloudMinds Launches XR-1, a Cloud-Based Humanoid Service Robot", [Online], RBR Staff, 28 February 2019, Robotics Business Review,
Accessed from: https://www.roboticsbusinessreview.com/service/cloudminds-launches-xr-1-a-cloud-based-humanoid-service-robot/ Last accessed: 28 March 2019

Japanese investments and technological developments behind social personal robots are well-known by academia and industry. Asimo robot, made by Honda, has been existed in the world of humanoid robotics for the last nineteen years. It is designed to "someday assist people in daily lives" and it has taken tangible steps closer to complete this statement. Only 130 cm tall and 50 kg heavy, could complete its humanoid look by completing many different tasks such as communicating in sign language, opening bottles, playing football. Asimo is not yet available in the market for personal use but could be a good candidate for being an HSR.

The above-mentioned products are yet not offered for personal use and they currently operate only for general tasks identified by the companies developing them. We believe that healthcare-specific robots will first be offered to personal use to revolutionize human life from the core. Specialized healthcare robots according to the person belongs to a specific demographic group (e.g. elders, children, etc.), type of disease (cancer or flu), types of treatments (in-bed or at home) could save people's lives, save time and offer comfort while they need medical assistance. However, it may come with many risks and costs, especially from the privacy point of view. As Fosch-Villaronga et al.[241] comprehensively addressed, the possible risks before privacy and data protection breaches of patients using or assisted by healthcare robots are various. For instance, they refer to the confidentiality of the health information or data of patients which are regulated by national laws and the GDPR in case of personal use of robots e.g. at home, or via a mobile app. The reason why they raise this issue is that the robot's capability to extract information regardless of the patient's will and out of her knowledge, share it with others, and eradicate the thin line between robot as a health care assistant and a living real organism like a human. As we will highlight in the following sections, their anthropomorphic outlook and behaviors ensure some level of trust which results as a relationship between humans and robots, like a human to human relationship. While the second issue is related to consent, so many possible actors operating the healthcare robot such as doctors, practitioners, nurses, hospital and many others especially manufacturers or companies that robot shares data for development purposes makes it hard to specify actual operational purposes of the robots and to find the exact data controller. In the following section, these problems will be analyzed deeper, but an overview of AI and robotics in the EU in general and in the sample countries specific will be first introduced to evaluate the current developments in these topics. This analysis is crucial to

[241] Fosch-Villaronga, et. al., 2018

see what stage do the sample countries stand in terms of the development, and in parallel with it, regulation of robotics.

IV. AI and Robotics in the EU

The AI expert Kai-fu Lee once stated that Europe would not even take a bronze medal in AI competition in the world giving as a rough reason that the EU is not home for the companies working with Big Data such as social media, or internet and mobile-based applications. Further, he thinks that Silicon Valley and China lead the AI sector because they are more liberal and research-oriented[242] than the EU which poses a protective and conservative attitude towards data share. EC's Digital Commissioner Mariya Gabriel[243] also approved this statement, during her speech at the AI Forum organized in Helsinki in 2018 by admitting that yet there are few large AI companies in the EU and they are facing a major skills shortage. Investments on and developments in the AI field remain based on MS-specific efforts during 2019. The UK is considered to be leading the EU in this field, however, even with the UK's huge contribution to the EU's current position in the AI market, McKinsey's report on AI private investments revealed that the EU in total invest was less than Asia and North America[244] . The EU lags behind the US by its number of AI players in the world and we must point the fact that most of those players are UK based companies[245]. EU's late AI awareness does not only affect the continent to be away from AI-related science and technology, but the lack of AI technologies costs some of the millions of Euro loss for Europe. Europe would earn some 2.7 trillion Euro into its asset pocket if it could develop AI in business[246].

For these reasons, the EC decided to increase investments in AI in the frame of Horizon 2020 program about 70% to 1.5 billion Euros by 2020 which was only 1.1 billion Euro during 2014-2017 period, and by this way, increase the private and public investment at least up to 20 billion euro by 2020[247]. For private investments, EC plans to invest in a total of 6 billion Euros for the 2021-2027 period[248] which would still be almost half of the current US

[242] "Interview with Kai-fu Lee", Carly Minsky, [Online], sifted.eu, 14 December 2018. Accessed from: https://sifted.eu/articles/interview-kaifu-lee-artificial-intelligence/ Last accessed: 28 March 2019.

[243] Opening speech of Commissioner Mariya Gabriel at AI Forum in Helsinki on 09 October 2018, [Online], Accessed from:https://ec.europa.eu/commission/commissioners/2014-2019/gabriel/announcements/opening-speech-commissioner-mariya-gabriel-ai-forum-helsinki_en Last accessed: 19 November 2019.
Also, the EC admits that AI market in Europe is underdeveloped compared to the US and lacks large data sets which is an essential for the development of AI. EC, 2018a, p. 7.

[244] Bughin, et. al., 2019, p. 40.

[245] How this picture would change deserves another research, since Brexit has just happened on the 1st of February.

[246] Ibid., p. 3.

[247] "EU to invest 1.5 billion euros in AI to catch up with US, Asia" Julia Fioretti, [Online], Reuters, 25 April 2018.

[248] EC, 2018b, p. 3.

investments. While the EU puts such efforts to make the AI market alive, no AI leading third country has planned either developing or making business within the EU.

There could be many reasons why the situation is in this way. For example, the GDPR impact assessment report on AI technologies published by the Center for Data Innovation in 2018[249] claimed that Europe's strict personal data rules on ADM and data collection raises some concerns towards the full exploitation of AI and prevents the continent from such exploitation[250]. We think that the claim might be true, not because the GDPR is strict, but because of foreign tech-giants' careful avoidance of complying with the GDPR's rules. Such a discussion is out of this work's scope, but an important outcome of this fact is that, without a common approach, program and even a regulation on AI technologies, the MS will have a room for acting autonomously especially on providing regulations (as the Netherlands and Finland have been doing so for the last two years). While the EU is being late for such regulation, the fact that many of the tech-giants in the field of AI are located in the US (and in China, North Korea, Japan, etc.) mirror the US culture/society where the data is coming from and those companies are subjected to different legislation, basically business-oriented ones, different from the rights-based approach the EU has[251].

Comparing to the EU's moderate failure in AI technologies, EU's investments and developments in the field of robotics draw a better picture. The EU is the second-largest region of industrial robots, falling a bit behind Asia, but getting ahead of America[252]. Specific to the service robots, we must indicate that the highest number of service robots are placed in the EU, leaving America and Asia behind[253] (nevertheless the two AI leaders China and Japan are in Asia, and Japan more urges upon producing social robots). Furthermore, EC announced that the EU intends to keep its leadership in robotics by increasing the investments of up to 700 million Euro. EU's strong emphasis on boosting embodied AI, or in other words, robotics, has already brought some tangible results through so many projects

[249] The Impact of the EU's New Data Protection Regulation on AI, Nick Wallace, Daniel Castro, [Online], Center for Data Innovation Available: https://www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/ Last accessed: 11 June 2019

[250] "Europe is about to lose the global AI race – thanks to GDPR", Nick Wallace, [Online], https://www.euractiv.com/section/data-protection/opinion/europe-is-about-to-lose-the-global-ai-race-thanks-to-gdpr/ Last accessed: 28 March 2019

[251] Cath, 2018, p.4.

[252] IFR, Executive Summary World Robotics 2018 Industrial Robots, [Online], Accessed from: https://ifr.org/downloads/press2018/Executive_Summary_WR_2018_Industrial_Robots.pdf.
Last accessed: 15 January 2020.

[253] Gudrun Litzenberger, IFR Press Conference 18 October 2018 Tokyo World Robot Summit, [Online]. Accessed from:
https://ifr.org/downloads/press2018/WR_Presentation_Industry_and_Service_Robots_rev_5_12_18.pdf. Last accessed: 20 December 2019.

funded in the frame of Horizon 2020 during the last couple of years. Among those projects, there is a significant amount of projects targeting development only of social robots. Furthermore, many projects have been finalized not only producing social robots but on regulating them in an ethical and legal meaning. Some of the examples below may help to understand the current level of knowledge on the regulation of social robots in the EU. There is yet no uniform AI strategy or policy in the EU towards focusing only on social robots (and probably will not be), but there are some MS specifically focusing on the development and regulations of social robots in their AI strategies. At the MS level, there is a variety of practices; some of the MS do have a strategy and planning on AI which also paves the way for the regulation of AI and social robotics. Some of them still at the infancy level which also draws them back from putting any tangible regulative idea about AI. In this case, next section will review the MS AI plans subjected to this work to see at what level they are towards AI regulation.

1. Regulation of Social Robots Through EU-Funded Projects

"One reason for Europe's strong position in terms of research is the EU funding programme that has proven instrumental in pooling action, avoiding duplications, and leveraging public and private investments in the Member States."[254]

In the EU, most of the robotic projects are supported by the EC through the so-called Horizon 2020 and FP7 EU research and innovation program. Those projects mainly focus on restricted topics such as human-robot cooperation at work[255], robot use at SMEs[256], and social robots assisting industrial robots[257]. Specific to the social robots, there is a significant number of projects completed in the EU[258] and we will refer only to a couple of projects that Italy, Finland, Netherlands, and Hungary (either alone or together) involved in.

[254] EC, 2020, p.4.

[255] ROBO-PARTNER Project official website. Accessed from: http://www.robo-partner.eu Last accessed: 20 December 2019.

[256] Factory-in-a-day official website. Accessed from: http://www.factory-in-a-day.eu Last accessed: 20 December 2019.

[257] EuRoC Project official website. Accessed from: http://www.euroc-project.eu Last accessed: 20 December 2019.

[258] MuMMer (MultiModal Mall Entertainment Robot) project differs from the others, unlikely all the projects funded by the EU in the fields of industrial and healthcare robots, this project aims to create an interactive and autonomous robot for shopping malls. Again, Pepper is the robot in subject, it will "work" in a shopping mall in Finland to serve customers at the mall. This project might be one of a kind targeting anybody without grouping them according to their health or any other status. Project official website accessed from: http://www.mummer-project.eu Last accessed: 20 December 2019.

Elder and children care are some of the initial topics in which the EU social robot projects focus on. For example, Culture-Aware Robots and Environmental Sensor Systems for Elderly Support (CARESSES)[259] project is an ongoing project aiming to build such robots assisting elders at home and also (with limited capabilities) outside of the home. The project initially aims to develop AI software that is culturally aware. Cultural competencies conceptualized by robots' awareness of cultural factors such as person's age, family structure, religion, and heritage; cultural knowledge such as person's beliefs, self-care practices, and health-related attitudes; and finally cultural sensitivity such as the person's language, accent, communication, and interpersonal skills, and trustfulness. These competencies are highly related to persons' private spheres (from their religion to the trust level), but no data protection concern was referred to on the project website. Moreover, with the help of these competencies, the robot could sense and understand a person's whole emotional and cultural map, then adapt, plan and execute actions according to a person's cultural background. Finally, it can shape its whole interaction plan for the future based on these inputs[260]. The experimental part of the project has not been done in any of the MS, but the trials will take place only in Japan and in the UK, as the project description noted. Choosing these countries for the testing field might be because of the fear of the GDPR's obligations, even though data processing activities aiming research and scientific purposes as such projects aim are eased the GDPR (Article 89).

Another current and ongoing project, Social Cognitive Robotics in the European Society (SOCRATES), aims to train 15 Ph.D. students in the field of social robots for eldercare. The project was held consortium-based, consisting of partners from different profiles such as academia, business, and industry. The students' task is to focus on uncovered areas in this field and offer solutions to the common problems wherever indicated. These problems are, for example, related to understanding elders' emotions by robots to improve interaction through developing DNN with unsupervised learning and to make robots understanding emotional statements. Besides emotion analysis, the project aims to reach the following outcomes: improving social robot skills to recognize and express intentions through algorithms, to improve robots' adaptation to its environment and learn from the user by interaction, and to find a proper design and model for the robot. Finally, the students conduct

[259] CARESSES Project official website. Accessed from: http://caressesrobot.org/en/ Last accessed: 20 December 2019.
[260] Bruno, et. al., p.7.

researches for improving robots' acceptance by human and work on some ethical solutions[261]. Since the project is ongoing, no ethical solutions have yet been raised.

Drawing an ethical and legal framework for social robots is one of the priorities of the EU, as the HLEGAI also indicated[262]. The INBOT project aims to understand and examine the acceptance of interactive robotics in the frame of developing ethical and legal frameworks. It does not focus on developing a technical framework for robots, rather focusing on developing social aspects of robots for humans. Besides the other partners, there are four Italian[263] and two Dutch[264] partners involving the project. Much more focused on the impact of robotics in the labor market and the effects of robots to the intellectual property law, but it is interesting to observe that no data protection issue was referred in the project's introduction video [265] where the project team members speak about ethics, law and use of humanoid social robots.

Among the above-mentioned projects, the Human-Brain project is one of the most comprehensive ongoing projects involving very specific scientific researches in neurosciences (including AI and robotics-related works) researching specifically on the ethics and legal aspects of AI works[266]. The project team works with an external Ethics Advisory Board and ethics rapporteurs whom the scientists consult with during their researches which sometimes reaches on biomedical researches with humans and animals[267]. The project is an important piece of practice on how data protection and privacy-aware researchers could continuously comply with both legal and ethical rules, and the consent rules, at the core.

After a careful and comprehensive analysis of the EU-funded projects related to robotics in the last 5 years, we are confident to say that the EU's close future social robotics outcomes will be visible in healthcare in general, and elder and children care in specific. We also realize that CEE countries are not involved with the EU robotics project. From those CEE

[261] Without extending the scope of this work, we refer the aims and deliverables in this project shortly. All aims recognized in the project could be accessed here: http://www.socrates-project.eu/research/ Last accessed: 20 December 2019.

[262] In June 2018, the group has delivered some ethics guidelines on AI and policy recommendations for ensuring trustworthiness of AI investments. Accessible here: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence Last accessed: 20 December 2019.

[263] Scuola Superiore di Studi Universitari e di Perfezionamento Sant'Anna, Università Degli Studi di Siena, Centro Ricerche Fiat, IUVO S.r.l.

[264] University of Twente, Universiteit Utrecht

[265] INBOTS - Interactive Robotics for a Better Society, YouTube. Accessed from: tyhttps://www.youtube.com/watch?v=Nt4qwcVc1o8&feature=youtu.be Last accessed: 28 December 2019

[266] Human-Brain Project official website: https://www.humanbrainproject.eu/en/ Last accessed: 13 July 2020.

[267] Stahl and Wright, 2018, p.30.

countries, we could realize only Poland[268] and Romania's[269] participation in the robotics projects at the EU level. There is no Hungarian partner who participated in an EU funded project, so far[270].

In this section, we presented the EU wide developments in AI and robotics from the financial and regulation-planning points of view by using some statistics and provided some examples from projects related to this field. In the following, AI and robotics in investment and regulation points of view will be presented specifically to the countries selected for the analysis. These examples also shall be read as the mains reasons why we chose Finland, Hungary, Italy, and the Netherlands as sampling countries particularly, besides their geographical representation and the level of investments on AI technologies.

2. AI and Robotics in Hungary

Hungarian scientists have been following the developments in the AI field since the 1950's both in theoretical and practical meaning[271]. However, and in parallel with the trends in AI history (dynamic AI winters-summers), Hungary could realize the power of AI and robotics only now, and has started putting significant efforts on AI researches and investments in both public and private sectors. Most of the initiatives with this aim were made by the Hungarian Government, followed by the private sector leaders and start-ups taking the lead towards developing AI technologies in Hungary. As an example of the Hungarian Government's efforts, the so-called Artificial Intelligence Coalition established in October 2018 could be mentioned. The Coalition was set to define Hungarian AI strategy and keep Hungary up-to-date in line with the global developments related to AI. Therefore, such strategies and the knowledge-gained through the events organized by the Coalition could put the country in a leading position in Europe[272]. One of the aims referred by the Coalition is

[268] The project was aiming to create an open source software to support robotic applications for elder care. It was accomplished in 2016. rapp-project.eu official website. Accessed from: http://rapp-project.eu Last accessed: 28 December 2019.

[269] Universitatea Babeş-Bolyai is one of the partners. Project aims to develop robotic solution that will be used as an assistant to children with autism. It was completed in 2019. Accessed from: https://www.dream2020.eu/consortium/ Last accessed: 27 December 2019.
Institute of mathematics Simion Stoilow of the Romanian Academy is one of the partners. The project aims similar to the Dream project, building acceptable and useful HRI for children with autism. Accessed from: http://de-enigma.eu Last accessed: 27 December 2019.

[270] The last check on the EC's website showed the EU-funded projects on Robotics dated on the 10 January 2020. EC Digital Single Market official website on Projects about Robotics. Accessed from: https://ec.europa.eu/digital-single-market/en/projects/76017/3586 Last accessed: 10 January 2020.

[271] Sántáné-Tóth, 2007, p. 75.

[272] Mesterséges Intelligencia Koalíció official website: https://digitalisjoletprogram.hu/hu/tartalom/mesterseges-intelligencia-koalicio Last accessed: 27 December 2019.

remarkable for the present work since it mentions speeding up the legal regulations on AI to pave the way for better developments in Hungary[273]. Altogether the Coalition has 147 members; 78 of them are international and Hungarian companies, and the rest consists of universities, research centers, and professional organizations[274]. Soon after its establishment, six working groups were defined under the Coalition, and one of the groups has started working on the regulation and ethics of AI[275]. It should be noted that there is yet no Hungarian national AI strategy adopted.

As we indicated before, private companies and startups yet lead AI developments in Hungary. Some of their fields of interest might be worth mentioning here to reflect which subcategories of AI developments are taken into consideration in Hungary that would later shape the future of Hungarian robotics. According to our research, it is obvious that driverless cars are one of the first robots that would raise in Hungary. For example, a company developing AI techniques to reach fully autonomous cars offers software for self-driving purposes, a simulator where driving experiences could be developed as if it is in real-life, and hardware for building neural networks for development[276]. Some of the international or multinational automotive companies also contribute to Hungary's AI developments. A German automobile company, which has been active in Hungary for years, opened its AI office in Budapest with the support of the Hungarian Government in May 2018[277]. The company invested in Hungary aiming to develop ML and other techniques to integrate the center in the global driverless car sector[278]. Further, an international test field for autonomous cars has been built in Zalaegerszeg[279]. Although the field is being used for

[273] "Megtartotta első plenáris ülését a Mesterséges Intelligencia Koalíció", Innovációs és Technológiai Minisztérium, [Online], 29 November 2018. Accessed from: http://www.kormany.hu/hu/innovacios-es-technologiai-miniszterium/hirek/megtartotta-elso-plenaris-uleset-a-mesterseges-intelligencia-koalicio Last accessed 4 January 2020.

[274] Ibid.

[275] "Hat szakmai munkacsoporttal kezdi munkáját a Mesterséges Intelligencia Koalíció", [Online], Digitális Jólét Program, 3 December 2018. Accessed from: https://digitalisjoletprogram.hu/hu/hirek/hat-szakmai-munkacsoporttal-kezdi-munkajat-a-mesterseges-intelligencia-koalicio. Last accessed: 4 January 2020.

[276] AI Motive official website. Accessed from: https://aimotive.com/products/#aiDrive. Last accessed: 4 January 2020.

[277] "Hungary joins EU initiative on artificial intelligence", [Online], Daily News Hungary, 10 April 2018. Accessed from: https://dailynewshungary.com/hungary-joins-eu-initiative-artificial-intelligence/ Last accessed: 4 January 2020.

The Government supported the company around 3.2 million Euro for R&D projects.

[278] "Mesterséges intelligencia: A Continental 2021-ig megerősíti az egész világra kiterjedő szakértői hálózatát", [Online], Continental, 12 November 2018. Accessed from: https://www.continental-corporation.com/hu-hu/sajto/sajtókoezlemények/mesterséges-intelligencia-151340. Last accessed: 4 January 2020.

[279] ZalaZone Official website. Accessed from: https://zalazone.hu/en/track-vision/the-essence-of-the-project/ Last accessed: 4 January 2020.

testing and developing traditional cars, scenario-based situations occurring in the future in smart cities could be later tested for better designing and developing autonomous cars.

We also noted that AI as a software in the service sector is a trending topic in Hungary. A chat service has been developed to serve customers in different sectors from banking to health care[280]. The developer company considered the GDPR by stating that its product is in compliance with the GDPR's Article 25 and this is an advantage of the company over the tech-giants, with their words[281]. We have not found any company investing in social robots in Hungary yet, but as part of a social AI, this chatbot could still be given as an example.

Finally, the healthcare sector in Hungary has shown some significant developments in robotics. The Antal Bejczy Center for Intelligent Robotics (iRob), organized under the roof of Obudai University's Research and Innovation Center, focus on different areas in the field of robotics such as health care, industrial robots, and telerobotics. Hundreds of publications, impactful national and international projects and events, and continuous research outputs have been generated at this Center[282]. Although R&D projects are not directly yet including social robots, there may be a possibility for the Center to focus on social companions in healthcare in the future.

In conclusion, AI technologies in Hungary are at the initial phases of development, however, there is a potential in the country to boost the developments technically. There is neither a national AI strategy nor another policy paper on the regulation of AI technologies that have been published in Hungary, even though there is a scientific novel work written by Hungarian experts on robolaw reflecting the Hungarian perspective and was made available in 2018[283].

3. AI and Robotics in Italy

In Italy, AI developments are on-going mostly via governmental support and plans. There are few private companies active in the field, but many public actors, such as universities, contributing to and conducting AI researches. These private companies sometimes get financial support from the Italian government, but mostly, work jointly within the EU projects.

[280] Cheqbot (fromer TalkAbot) official website. Accessed from: https://cheqbot.com/ Last accessed: 4 January 2020.

[281] Akos Deliaga, "d!talk Talk Ákos Deliága, Talk-A-Bot Kft.", YouTube, d!talk, 17.05th minute. Accessed from: https://www.youtube.com/watch?v=I5IYSb_Hm_0&t=1025s Last accessed: 4 January 2020.

[282] Óbuda University, 2017, p. 31.

[283] Technológia jog – Robotjog – Cyberjog, 2018.

Robotics in Italy has already been a hot topic and creating social robots in Italy is one of the aims of the Italian Institute for Technology (IIT). It is safe to state those social robots that are human-centric, sympathetic, friendly, and ready to understand human behavior[284] being developed at Italian laboratories. They will soon assist humans in healthcare, environmental protection, and eldercare, as claimed. Moreover, those robots have been developed as a great example of collaboration and cooperation between the public, private, and academic sectors. Humanoid social robot iCub is an example of such a state of art, which has been developed at the IIT laboratories and already has built-in 36 copies. It is foreseen by the IIT that robots like iCub will not only remain at the laboratories or industrial sector but will become a part of Italians' daily life at affordable prices[285], thus it is possible to meet social companion robots at Italian homes soon[286].

Besides the technical developments, there have been several policy papers prepared in Italy aiming at the regulation and development of AI technologies. For example, the Italian Ministry of Economic Development published a call for 30 experts in AI field on 14 September 2018 to set a group of expert that will draft an AI National Strategy[287]. According to the call text, National Strategy would address several issues but also "a comprehensive review of the legal framework with specific regard to safety and responsibility related to AI-based products and services"[288]. Thus, it is not clear from this statement whether National Strategy will concentrate on data safety and issues related to liability occurring from AI technologies. There is no other task or goal specified neither for the group nor in the Strategy regarding data protection and privacy issues in the field of AI. Since there is no deadline specified for publication of the draft, the situation is expected to be clear in the future.

Following the global AI developments, the Italian digital agenda has also been updated consisting of a three-year plan focusing on improving the use of AI services in Public Administration. The agenda set "the Artificial Intelligence Task Force at the service of citizens"[289] under the Agency for Digital Italy (AGID). The Task Force's first aim was to publish a White Paper in which was published in March 2018. The White Paper focuses on

[284] For example, one of the priorities of the group on robotics research organized in the Italian Institution for Technology is creating robots with social cognition.

[285] Istituto Italiano di Tecnologia, IIT 2018-2023 Technical Annex, p.1. Accessed from: https://multimedia.iit.it/asset-bank/assetfile/11121.pdf Last accessed: 31 January 2020.

[286] Ibid., p. 7.

[287] "Artificial intelligence (AI): call for experts", [Online], Ministry of Economic Development, 14 September 2018. Accessed from: https://www.sviluppoeconomico.gov.it/index.php/en/news/en/202-news-english/2038605-artificial-intelligence-ai-call-for-experts Last accessed: 20 November 2019.

[288] Ibid.

[289] AGID, 2018, p. 16.

how to make AI useful to serve citizens in the public administration and what are the current obstacles before achieving this goal. The statement indicated that AI-based public services could decrease bureaucracy in public administration, therefore the citizens could save time and money while reaching the regular services. Healthcare, education, environmental protection, inter-administration information sharing, employment, transportation, taxation, and security could be some of the initial fields where AI services would be offered in a close future in Italy. The White Paper mentions the "use of robots to take care of the sick people"[290], in line with the current trends in service robots. Italy is ambitious for catching the global trends and leading Europe on developing Humanoid and Companion Robots (in other words, social robots), as the group on robotics research stated so[291].

The White Paper further examined the ethical aspects of AI, the role of data in AI, and the legal context of AI technologies specific to the Italian case. Possible risks in biased decisions and machine errors concluded the role of data problems. Personal data protection and privacy of citizens using AI-based public services were addressed only in the Legal Context section of the White Paper. We found this statement proper since the White Paper calls public administrators to encourage citizens to personalize their services, meaning that Italian authorities are aware of data protection risks before personalized services. Referring back to the Legal Context, it is clearly stated that collection of citizens' data should not cause pervasive social control and to avoid that, Article 25 Data Protection by Design and by Default, Article 35 Data Protection Impact Assessment, and consent mechanism referred in the GDPR was referred as a solution. There is no further recommendation referred related to personal data protection but this White Paper is the only document evaluating personal data protection aspect such a specific way, in comparison to the papers generated in other sample countries'. There is only a general recommendation suggesting to involve related actors in AI-based services from projects' pilot phase for ensuring transparency. In this case, we could summarize that the AGID evaluates the GDPR as a sufficient legal solution for the issues related to AI.

To sum up, there are many strategy and policy papers have been published in Italy supporting the technological developments in the AI field, including social robots. Ethics and legal

[290] Ibid., p. 6.

[291] The group has already received 138 patents and currently 17 patents have been under procedure. They completed 3 European projects, and are planning to raise these numbers soon by putting some weight on the academic trainings and launching new laboratories.

considerations together with personal data protection issues were also involved within these documents.

4. AI and Robotics in the Netherlands

Unlikely Italy and Hungary, several Dutch companies are serving a strong digital infrastructure (processing also a high amount of personal data) such as booking.com, and Viber and the country attracts some of the international companies e.g. Netflix since it has a well-established digital infrastructure providing cloud services and high-quality connectivity[292]. For many years, ADM systems have been used by the tax authorities, police, anti-fraud agencies, and immigration officials to prevent and predict illegal activities. AI in the Netherlands is a hot topic and regulation of AI technologies also is on the agenda of the Dutch Government. Several initiatives and documents have been raised describing the AI technologies in the Netherlands. We will present some of the important documents addressing the issues related to AI technologies, following.

In June 2018, the Dutch Ministry of Economic Affairs and Climate Policy released the Dutch Digitalization Strategy expressing the government's plans on preparing the country for a better digital life. To structure the future of digital life in the Netherlands, the Dutch government states that, "privacy protection, cybersecurity, digital skills, and fair competition" should be strengthened[293]. Besides defining clear steps towards the future of digitalization in the Netherlands, the government emphasizes on its guarantee of protecting fundamental rights and values, such as privacy. It identifies and recognizes the problem of how do people insufficiently give consent to the companies even though the GDPR is in force[294]. To solve such issues, the Dutch government stresses the importance of data self-management by data subjects which would enhance the trustworthiness of the digital systems. According to this view, data subjects should be able to exercise their rights granted in the GDPR fully, and data controllers and processors should be well aware of their responsibilities. In the eye of the Dutch government, companies have an important responsibility to increase the trust of people towards their AI-based products. Finally, the paper evaluates the transparency rule, not from the data protection point of view directly, but the consumer's rights point of view. According to the paper, users of AI technologies

[292] Dutch Digitalisation Strategy, 2018, p. 16.
[293] Ibid., p.8.
[294] Ibid., p. 40.

should always be ensured with their right to know whom to contact in case there is a problem with the purchased product.

Another way of strengthening privacy protection, according to the Dutch government, is to "work with the people concerned on practical framework and solutions."[295] Since the strategy paper was released, the government took tangible steps to fulfill this statement. For example, AI Coalition in the Netherlands was launched on the 8th of October 2019 with 65 partners including companies, governments, civil society organizations, and universities. The Coalition's first aim is to catch up with the US, China, and other AI leading countries in the AI investment and make the Netherlands an AI-forerunner in Europe. This Coalition adopts the "AI for everyone" slogan, meaning that human is placed in the center of AI developments in the Netherlands[296]. Boosting privacy-friendly digitalization by investing in more interdisciplinary researches is an embedded aim in these investments. In this way, more knowledge could be created which then could reinforce better policymaking. Education and life-long learning are also an integrated element of a healthy digital environment[297]. Boosting interdisciplinary researches and life-long learning strategies are also some of the solutions we will refer at the end of this work. During our research, we realized that the Dutch government and its organs are highly coordinated in regulating AI technology in the country.

In November 2018, the AI for the Netherlands report[298] was prepared by several public and private contributors such as the Netherlands Organization for Scientific Research and the Innovation Center for Artificial Intelligence. Some resources[299] call this report as a Dutch National AI Strategy, but since it is not announced by the Dutch Government so, and the English translation of the foreword explicitly states that the report was prepared as "a booster of a national AI strategy", we believe that it could not be fully understood as a national strategy. However, the work draws a comprehensive picture of the Netherlands' position in the world in terms of AI technologies and highlights some solutions to bring the country up to the level of AI-developed countries.

[295] Ibid., p. 13.

[296] "AI coalition wants algorithms to work for everyone", [Online], Eindhoven University of Technology, 9 October 2019 Accessed from: https://www.tue.nl/en/news/news-overview/09-10-2019-ai-coalitie-streeft-naar-algoritmen-voor-iedereen/ Last accessed: 10 October 2019.

[297] Dutch Digitalisation Strategy, p. 30.

[298] AGID, 2018.

[299] "AINED: A National AI Strategy for the Netherlands is Published", [Online], Amsterdam Data Science, 12 November 2018. Accessed from: https://amsterdamdatascience.nl/news/ained-a-national-ai-strategy-for-the-netherlands-is-published/ Last accessed: 28 January 2020.

There are two important AI-related organizations in the Netherlands that we would like to mention. One of them is the Innovation Center for Artificial Intelligence that is an initiative brought by the University of Amsterdam and Vrije Universiteit to involve industry, academia, and the government to boost AI knowledge to contribute to the innovation and development of AI in the Netherlands. There are nine labs available to produce such knowledge in four Dutch cities namely, Amsterdam, Delft, Nijmegen, and Utrecht. All the labs are established with the support of the stakeholders from industrial leaders (e.g. Bosch, Qualcomm, ING) to the leading universities in those four cities, and also government actors such as the National Police. Each lab focuses on different sectors, such as healthcare, retail, finance, education, and national security[300]. The Center hosts some of the important researches focusing on developing AI knowledge and contributing to the national AI development.

The second important organization is the Alliance for Artificial Intelligence (ALLAI) that was organized by the three Dutch members of the EU's HLEGAI to spread the idea of creating responsible AI in every aspect of human life[301]. ALLAI now offers a Responsible AI Program consisting of different modules focusing on different aspects of AI implementation on human and social life. These modules include technical, societal, ethical aspects of AI or AI-centric policymaking, but for us, the most significant part of these modules is their focus on separating the ethical aspect and legal aspect of AI from each other. Since our research experiences show that especially industry but also academia intertwine law and ethics in the case of AI regulation, ALLAI's approach stands as a unique approach.

Specific to the robotics in the Netherlands, there are different types of robots have been developed in several sectors such as health-care, industry, safety, food and agriculture, and consumer services fields[302]. Social robots have mostly been planned for the healthcare sector however, creating robots for personal use not yet an issue in the Netherlands; though is a

[300] The Innovation Center for Artificial Intelligence official website. Accessed from: https://icai.ai Last accessed: 28 January 2020.

[301] Alliance on Artificial Intelligence official website. Accessed from: https://allai.nl Last accessed: 28 January 2020.

[302] Robotics in the Netherlands, n.d., p. 8. Shadana Innovation Management and Consultancy report prepared for the State Agency for Enterprising [Online]. Accessible here: https://www.araneo-magna.nl/images/pdfs/Robotics-in-the-Netherlandsfinal.pdf

planned action according to the Dutch Digitalisation Strategy[303]. From universities[304] to private companies[305], several labs and projects are focusing on developing social robots.

All in all, we could indicate that there are much AI-related cooperation and collaboration opportunities available in the Netherlands. Dutch academy and industry keen on creating opportunities contributing to AI developments in the country. The Dutch universities are the engine behind producing AI knowledge in the country. Many Universities either alone or jointly with others improve the Netherlands' AI knowledge hub. The industry supports AI-related initiatives and public institutions connect the AI-related communities. It is worth mentioning that the Dutch government is cautious about the full application of ADM in the Netherlands giving as a reason that the rules in the GDPR remain general to regulate such a specific field that may risk fully protection of fundamental rights. The Ministry of Interior and Kingdom Relations coordinates several departments on reporting the possible issues arising from this fact and we believe that there soon will be an AI policy paper(s) in the Netherlands (if choose not to wait for the EU), including a specific data protection section. Currently, the Dutch Data Protection Authority announced[306] that there will be a risk-based supervision launch on AI services offered by the companies based on the amount and type of data they process until 2023. The Authority also will offer supervisory instruments, such as on the interpretation of standards, giving legislative advice, providing information and tips about the enforcement to the companies and public institutions offering AI-based services. Although the year 2023 might be too late for such supervision, especially taking into account the country's ambition on developing AI-based services, it will generate some positive results.

5. AI and Robotics in Finland

Finland made one of the first statements in the EU on making AI technologies an integral part of the country's development strategy. In March 2017, Finland launched the Artificial Intelligence Program under the Ministry of Economic Affairs and Employment. The related Minister immediately formed an AI working group assisted with four specific subgroups

[303] Ibid., p11.

[304] For example, Eindhoven University of Technology operates a Social Robotics Lab; Tilburg University hosts a department of Social Robotics and Language Development.

[305] LEO - Center for Service Robotics Official website. Accessed from: http://www.leorobotics.nl/ Last accessed: 28 January 2020.

[306] "AP legt focus in toezicht op datahandel, digitale overheid en AI", [Online], Autoriteit Persoonsgegevens, 11 November 2019. Accessed from: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-legt-focus-toezicht-op-datahandel-digitale-overheid-en-ai Last accessed: 25 November 2019, thanks to Mr. Paul Severens for drawing our attention to this information.

that comprehensively evaluated Finland's AI readiness, the problems, the strengths, and the weaknesses in adopting AI technologies in Finland. The subgroups were formed under four thematic areas, namely, Competence and Innovations, Transformation of Society and Work, Data and Platform economy, and the Ethics group. Comparing to Italy, Hungary, and the Netherlands, Finland has the only ethics group evaluating the AI technologies from this specific point of view, including privacy.

AI working group made the first evaluation on Finland's AI status and released the first AI strategy paper concluding eight statements reflecting Finland's roadmap to make the country leading in Europe. Later in 2019, these eight statements were updated and increased to eleven statements. The strategy reflects Finland's positive evaluation of AI technologies to be used at businesses, the public sector, for citizens and society[307]. It is at the utmost importance for Finland to take the opportunity of AI technologies in the industry which then could contribute to growing the country's export[308]. Besides the benefits of AI to the country, the citizens' and society's involvement with AI was also mentioned. For example, it was stated that every Finn's daily life would be surrounded by (an ethical and open) AI technologies within the five years[309], and this would most probably be first in the health care sector.[310] Besides the health-care, education and transportation together with energy and security would be the planned AI services for the citizens and society.

The Finnish approach to AI is not only software-based; it also includes robotics as an important part of AI. Although no specific mention was made on social robots[311], the strategy paper released a plan for developing robots to facilitate better wellbeing for the people in Finland. Also, a note was made on using robotics in the service sector, and health care services on the top priority[312].

The AI working group further reported that the adoption of AI-based services by the citizens could be easier in Finland since the population in Finland holds a high level of education

[307] FMEAE, 2017, p. 13.
[308] Ibid., p. 23.
[309] Ibid., p. 14.
[310] Ibid., p. 24.
[311] Although social robots in Finnish society have not yet taken full space, there are some pilot projects engaging them in their life. For example, a humanoid social robot appeared at some schools in Tampere as a language and a math teacher assistant in frame of a pilot project. "Techno teachers: Finnish school trials robot educators", [Online], Reuters, 27 March 2018. Accessed from: https://www.reuters.com/article/us-finland-school-robots/techno-teachers-finnish-school-trials-robot-educators-idUSKBN1H31XT. Last accessed: 1 February 2020.
[312] FMEAE, p. 27.

there is AI education available in the country[313]. Empirical works are supporting this prediction, for example, a study reporting social robots could be an opportunity for people in Finland to continue their independent life and indicating half of the citizens in Finland would accept a care robot assisting them in daily routine activities[314]. According to the panel discussions launched by the authors, citizens expect to "be informed and educated on robotics-related matters before the larger introduction of care robots in care services", besides their other expectations.[315]

The working group also highlighted the importance of the principles of transparency and accountability as aspects of forming a good AI society[316]. Remarkably, it was noted that the principles mean different for the different actors in the AI field, from the companies to the citizens, requiring the country to make a uniform definition of those principles. This statement shows the importance of having a national strategy to define the terms and targets clearly, especially in a specific field like data protection. Finland has a distinctive point of view from the other countries in this sense.

Finally, as noted before, the Finnish strategy concluded eight recommendations of the working group for leading Finland an AI leading country. One of those recommendations is noting the impossibility to solve the ethical questions completely, but suggesting to collect the different viewpoints, including citizens' opinions for a start[317]. With this vision in mind, the Final Report of Finland's Artificial Intelligence Programme that was released in 2019 brought a more comprehensive and deeper analysis of the case.

The Final Report chooses sample AI companies operating in Finland and developing AI basis services, from transportation and carriage to customer services, and innovation, intending to describe the current situation in the country. It is because the Ministry of Economic Affairs launched Finland's Artificial Intelligence Accelerator project aiming to assist companies with a specific portfolio to guide them since the first report[318]. With the help of this project, it was possible to see in which fields AI is operating in Finland. Consumer services is one of those fields, however, we realized that the report points to a very specific privacy issue without further elaborating in detail. The report mentions a

[313] Ibid., p. 32.
[314] ROSE consortium, 2017, p. 14.
[315] Ibid. p. 28
[316] FMEAE, p. 40.
[317] Ibid., p. 60.
[318] There are 29 companies joining the project as of 1 February 2020. Accessed from: https://faia.fi Last accessed: 1 February 2020.

company collecting a large amount of data on consumers' shopping habits to recipe recommendation service, besides recommending foods for the next shopping. An informative box placed in the final report[319]does not mention much about how the company protects the privacy of consumers in the subject.

In the Final Report's next sections, each key action was evaluated based on the first report and we will only mention data protection related evaluation of each. Data and personal data were one of the topics mentioned in each action, for example, enabling access to data held by different actors was among the plans. The plan further mentioned that rules for accessing and secondary use of data should be clarified to complete the key action successfully[320]. The report also noted that there were specific acts enacted for particular government services processing personal data (e.g. the Koski service operated by the Finnish National Agency for Education to trace students' qualifications and achievements) to the proper operation of those services in line with data protection rules, such as acts enabling consent management tools to ensure the legal operation of the service[321].

Such acts are not the only tools used in Finland to strengthen the protection of personal data and privacy. There are practical steps taken by the Finnish government and to our knowledge, there is no such an example encountered in Italy, Hungary, and the Netherlands. The first International NGO for data protection called MyData Global was established under the Ministry of Transport and Communications to promote an individual's autonomy to manage their data. The organization has its roots back in 2018 based on the initiation of a couple of individuals aiming to promote informational self-determination principles throughout the globe. An electronic tool called MyData offered to the individuals' use to help them manage their data in the connected world based on the principles also referred to in the GDPR, but primarily on consent management[322]. It also offers an API that companies could use to access datasets in one platform without violating the right to data protection[323]. These tangible privacy protection tools available in Finland differ the country from the other three countries subjected to analysis in this work.

[319] FMEAE, 2019, p. 40.
[320] Ibid., p. 52.
[321] Ibid., p. 57.
[322] Finnish Ministry of Transport and Communications, "MyData: A Nordic Model for human-centered personal data management and processing" [Online] Accessed from: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=y Last accessed: 1 February 2020.
[323] p.11

The last observation regarding the Finnish approach related to AI and personal data protection is the statement of ethics as a key action steering AI development into a trust-based and human-centered direction[324]. During the past two years following the first report, many works have been done to identify the challenges regarding ethics and human rights protection specific to the development of AI in Finland. For example, discussions took place with Finnish organizations, an evaluation was made on public sector activities and consultations were made with the HLEGAI by the Finnish government. But the most important action, in line with the suggestions made at the end of this work, was about launching the online public course[325] by the University of Helsinki focusing on teaching and raising awareness on ethics, rights, and responsibilities of the people interacting AI. This online course platform transfers a high level of technical and legal information specific to AI, simply and engagingly to the public. The platform is also available in English.

Finnish example reflects that much more could be done with simple and practical actions rather than focusing on the codification of formal rules and principles in legislation. However, to do that, it is important to identify what exact areas do the legislation leaves room for simple and practical applications for the actors engaging with AI.

6. Summary

The descriptive analysis made on the EU and four sampling countries specific in terms of their level of development in the AI and robotics shows that, although the countries stand in different levels in terms of investment and regulation of AI, a certain degree of the technology is present and there are attempts to regulate it.

Finland, both in technology and regulation point of views, is leading among the other sample countries. The Netherlands follows Finland while Italy has shown efforts to catch up with them. Hungary crawls around developing the structural and financial necessities to raise the level of investments and researches, however, there is no attempt noted in terms regulation. In this case, this work represents the feedbacks of those experts from the different EU MS taking different actions in terms of investment, research, and regulation of AI technologies. Following, the problems related to the applications of the GDPR on robots will be presented as a result of the comprehensive literature analysis conducted both in the legal and technical literature.

[324] FMEAE, p. 102.

[325] See: https://course.elementsofai.com Last accessed: 1 February 2020.

V. HSR and Data Protection: Problem Statement

People today share their personal issues with electronic systems bravely. They do use electronic calendars, emails, text messages; leave call logs, personal documents, browser histories, financial data, location data and many more to the machine evaluation. They are very generous about sharing their issues with machines without knowing that what they share with machines could easily (and rapidly) reach to indefinite places, machines, and persons. In this way, big data, data mining facilities, and easily accessible personal data remove the obstacles standing in the way of social robot's data collection. Some numbers could help us to illustrate how uncontrollable it is to spread and manage personal data today. For instance, the IDC analysts predict 33 zettabytes of data available in 2018 to increase up to 175 zettabytes of data in 2025 in data storage such as cloud, smartphones, IoTs, or at cell towers. If one has a mobile phone with the capability of 64 gigabytes local storage, and if all of it is to be used, it is possible to imagine how many pictures, documents, videos, or voice records are enough to fulfill only 64 gigabytes, and how much of such data is needed for fulfilling that 33 (or even 175) zettabytes of space[326]. The number of connected devices, such as computers, mobiles, cameras, etc., producing such an amount of data is estimated at 30 billion in 2020 to be 75 billion in 2025[327]. In addition to voluntarily data share, the internet and social media grow every day with the help of personal data and become a treasure chest for the development of the AI technologies, as well as become a meeting point for data exchange of connected devices. Such a growth, unfortunately, leaves out scrutiny procedures necessary to ensure accountability and transparency[328]. People adopt these technologies without really knowing the disadvantages or possible risks behind them. Robots or other personal AI services, in the end, could collect data from other IoT devices which may suddenly become widespread for personal use at homes, or public spaces such as cities, workplaces, without knowledge of or understanding by data subjects.

The life-force of the robots, their blood is without a doubt, data. With the power of data, a social robot can see, hear, understand[329], learn, plan, reason, negotiate to solve problems[330],

[326] Reinsel, Gantz and Rydning, 2018, p.3.

[327] Columbus, L. "Roundup of Internet of Things Forecasts and Market Estimates, 2016", Available at: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#6a558beb292d Last accessed: 20 June 2017.

[328] Kemper and Kolkman, 2019, p. 2038.

[329] Microsoft, p. 32.

[330] Open source code developed by Facebook's Artificial Intelligence Research labs was evaluated as "an important step for the research community and bot developers toward creating chatbots that can reason, converse, and negotiate". Available at: https://code.fb.com/ml-applications/deal-or-no-deal-training-ai-bots-to-negotiate/ Last accessed: 18 October 2019.

recognize voices and faces, process languages, make decisions, guide its interaction with a human[331] socially and emotionally, shortly, simulate human. The source of such data could be both based on the data related to past activities of the users or data based on real-time activities of the users such as their weblogs[332]. Advanced hardware equipment supports direct data collection from the robot's environment. Robotic eyes that are supported with High-Definition cameras help them to analyze its environment visually. Mouth (speaker), ears (microphones), and other physical pieces (arms, legs, head, etc.) could enhance the robot's environmental perception and interaction. In addition to physical equipment, their computation capacity paves the way to make abstractions from the big amount of data to make it meaningful and easy to process within seconds[333]. A social robot may collect different types of data (personal data and special categories of personal data) such as biometric data, location data, voice and images, health and medical data, conversations,[334] opinions, emotional expressions, and more, at once. As a result, a social robot can collect, process, organize, and store data and it could do so promptly. It would not be wrong to say that the AI is on the peak of its evolution as we currently understand it and it owes this to data.

Bearing in mind all above statements, a robot could collect personal data from:

- Internet or devices that it connects through the internet,
- Oral communication such as questions and requests or conversations,
- Through its hardware and sensors with the help of its analyzing capability of human behaviors, or other devices attached to the robot, such as IoT devices.

In conclusion, it is safe to state that, any data from any resource could be a part of ADM and the next section will present what types of personal data are protected by the GDPR. Then, what specific type of personal data a social robot could process different from other technologies will be mentioned, that is raising many questions specific to the use of social robots at the households.

[331] Kamarinou, Millard and Singh, 2016, p.6.
[332] Alpaydin, p. 13.
[333] Li, X., Jiang, H., p.383.
[334] Kerr, 20015, p.8.

Section 1. Conceptualization of the Problems Based on the Definitions in the GDPR

This section is going to present the primary relationship between AI and GDPR based on the basic definitions and rules referred to in the GDPR. Without presenting this relationship, our analysis would be structurally incomplete since the main aim of this section is to prove how personal data becomes the main element of AI technologies from the data processing, profiling, and ADM, and actors involved in the processing point of views. The secondary relationship between these elements will be presented in Section B where we analyze the possible concerns regarding practicing the consent rule specifically.

1.1. Personal Data in the GDPR

Regarding the types of personal data, a social robot could process, there is no list we could concretely present here; since no data is left without being processed in terms of current technologies. A type of data referred to in this statement is law specific, which is based on the definition of personal data referred to in the GDPR (however, there is no limit in here either, as we will soon prove). The definition of personal data in the GDPR comprehensively is related to all those types and forms of data a social robot could process. Article 4 of the GDPR defines all the terms used and starts with the definition of personal data, which is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". The EU lawmaker makes specific definitions for certain types of data, which was called sensitive data in the Directive 95/46/EC and special categories of personal data in the GDPR Article 9 (1), in order not to leave any room for misunderstanding or misapplication. These types of data are, genetic data, biometric data, and data concerning health, all are safeguarded in a more specific way in the GDPR. If the data subjected to the processing activity is sensitive, the data controller[335] is not allowed to process without, for example, explicit consent of the data subject[336].

According to the GDPR, emotions, financial status, physical appearance, data related to personal health condition, biological and physiological data, and processing of any other similar type of data fall under the scope of the GDPR. It is evidential, that all the data introduced to a social robot could be personal data or already collected data that could easily be transformed or linked to personal data[337]. Moreover, an AI system could easily transform several personal data into sensitive data; it could easily guess people's religion, which is sensitive data in the frame of the GDPR, from people's online food or cloth choices.[338] AI could interfere with someone's religion only by processing their pictures (e.g. woman in a scarf, a man wearing a kippah). Further, it could make an abstract estimation about a person with stuttering (or a different kind of speech disorder) during the interaction, via the speech-recognition function. However, what if the initial purpose of the algorithm was not identifying such disorders or people's religion? Finding out whether a robot is processing data for the purposes that it was created for is not an easy task, as Rhoen and Feng indicate, that "it is impossible for data subjects, data controllers and national supervisory authorities" to detect the outcome of a data processing activity that may not be intended directly by the programmer, but has happened because of the algorithm's ability to reach sensitive data by combining a couple of personal data.

Another example could help us to explain how algorithms may not remain within the borders of a single purpose when there is sensitive data to be processed, for example, biometric data is subjected to the collection and processing by a social health care robot. Štitilis and Laurinaitis define two major biometric categories that a robot could perceive easily: physical and physiological data such as iris, ear shape, face, and palm outline, and data related to behaviors such as person's signature and keystroke patterns[339]. Data such as face and voice, ear shape, fingerprint, palm, etc., are being used initially for identification purposes since

[335] According to the GDPR, there is no difference between a natural person and legal persons by means of obligations and responsibilities as a data controller. The definition refers the data controllers as "thenatural or legal person (emphasis added) alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

[336] There are several occasions in which the data controllers could be allowed to process specific personal data. We excluded the other conditions since this work focuses only on consent obligations.

[337] Karyda, et. al.., 2009, p. 201.

[338] Rhoen and Feng, p. 147.

[339] Štitilis and Laurinaitis, 2017, p. 619.

they do not change and do have a distinctive character and ensures time and cost-efficiency. If someone’s biometric picture is registered in a certain system, that person can be identified by other systems using biometric data processing techniques. While this example is still applicable to the case of shared databases, we consider the possibilities of a single personal social robot collecting such physiological and psychological data to adjust itself according to the user’s personality. In this case, for example, the voice of the user being used for authentication could be indeed processed for predicting whether the user caught a cold without explicitly indicated before.

Finally, since we used the term algorithm several times previously, we would like to explain the algorithm and its relation with personal data processing. The algorithm could be defined as "a series of instructions for performing a calculation or solving a problem, especially with a computer[340]”. The instructions are applied automatically on the available data to reach conclusions about them. These instructions could be bits of codes written by human developers, or as it is the case in a demanded future, could be simulated by the machine itself. Algorithms value any data regardless of its usefulness[341], and it does not matter what type of data is subjected to the algorithmic evaluation; they are not aware of such concepts. Types of data only matter in case of legal applications (personal data-specific categories) for the data controllers or processors operating or using the algorithm. As much as the algorithm is developed, a social robot could make broader interpretations counted almost equal to (or sometimes even better than) human evaluations. Millions of examples used for training the algorithms with specific ML techniques process any type of data without differing between data categories defined in any legislation.

Application of algorithmic models on personal data absolutely would result in a discovery of new personal data, even though such data is not yet defined as personal data in the EU legislation. Either the input data or the output data generated as a result of profiling should be identified as personal data. Because the algorithmic output is new information about the individual (e.g., 90% probability for cancer diagnose of the individual), to our view, since algorithm operates to know the unknown personal aspects of the individuals. In case the inference might be a yes or no, or a quantile or percentile, they point specific personal information (Does she have skin cancer? 90% probably yes).

[340] House of Loeds, 2018, p. 14.

[341] van den Hoven van Genderen, 2017, p. 12.

A social robot collecting personal data may evaluate that data with an advanced algorithm could offer personalized services to the users. There is no doubt that people wish to leave certain works at the hands of robots to have more free time today[342]. They wish to have a better life, a healthier life[343], and they know that it is possible with robots with AI. However, it may not always be possible to put clear borders on data processing activities in AI systems making the data subjects may not always be aware of the risks behind the processing of their data, and one reason for that might be the deceptive trust that data subjects put in social robots.

1.2. Personal Data Disclosures

During the making of this research, it was obvious for us to conclude that the social robots differ from others because they can interact with a human in every way which encourages them to share data with robots in every way. Although there are discussions among the researchers (especially, the members of social sciences) claiming that AI cannot outperform human, because it will never be like a human, "AI itself claims that it can behave similarly to persons/human" by creating "machines with the mind"[344]. Either it could outperform humans or not, the machines with mind simulating humans may create a misperception of these robots. As a consequence, humans may trust robots which are the key for data controllers to enter into even the most private spaces, such as, homes, and manage their life without being aware of the consequence of this invitation. Once they enter homes, an endless HRI may cause unintentional data disclosures[345] both by the user and the others sharing home. Trust is indeed necessary for people to accept and use AI[346], but not in this way. Trust is a psychological necessity for human and there might be many reasons why human trusts robot as LaRosa and Danks[347] group those reasons into three categories. A human may trust

[342] Eurobarometer, 2015, p. 4.

[343] Indeed, privacy risks are not limited to social robots. For example, Fosch-Villaronga et.al (2018, p. 113) gives the exoskeleton example, which the workers wear for operating the robot that they could execute their job better, but also cause collection of workers' personal data and profiling the worker. While a worker would interact with the robot only within work-related purposes, the collection of workers' health-related data is also possible. Once again, the choice of a social robot in this work is the sample and is the way of specifying the scope of this work.

[344] Nath and Sahu, 2017, p. 2202.

[345] Actually, in some cases, a constant HRI might be very useful for, e.g., treatment of dementia. As long as human spends time with the interaction, treatment will be more successful. However, the danger, in this case, is about integrating robots in people's daily life so seamlessly that they cannot even realize what they share with robots.
Ibid., p. 2201.
See also, Fosch-Villaronga, 2018, p. 101-105.

[346] EC, 2018, p. 8.

[347] La Rosa and Dank, 2018, p. 211.

a robot just because of the roles defined for it (role-based trust). A health-care robot, just like doctors, could be found trust-worthy just because they receive good care from the robot. Behavioral trust occurs, when, for example, a home robot does take care of the home well, and executes all the tasks without or with a few mistakes would gain the trust of users. Finally, a human may trust a robot just because it could predict its actions (understanding trust). Unpredictability is not questioned in this case, and we think that this type of trust should exist between social robots and data subjects. Humanoid look, in each category, plays a crucial role in building trust that leaves the data subject in an uncanny valley, the main reason why data disclosures would be so easy.

The term uncanny valley belongs to the (social) roboticist Masahiro Mori[348] who used it for the first time in his Japanese publication about forty years ago. Mori made a strong relationship between the human deception and mathematical functions (when the value x increases, the equivalent y also increases) and conceptualize the deception in 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 clearly, as long as the robots will be designed in a way they look or act like human (f(x)), human will produce such feelings (e.g. affection) towards robots (y) preventing from perceiving them as machines. As the humanoid design increases, the humanoid perception of robots will also increase (f(x)=y). Personalization of robots through RL techniques, on the other hand, directly affects people's perception of a (social) robot; as personal as the robot is, the user's perception of humanoid companion increases. Such perception may emotionally manipulate people, hence, people may even think that a robot can have emotions[349]. People's emotional engagement with robots encourages them to disclose more personal information for functional rewards. When functional personalized rewards combine with a humanoid outlook, people may collaborate with robots more, since they think that robots are human, because they act and look like a human[350]. Persons living with social robots will be required to share personal data if they wish to receive personalized services, however, illusionary perception of the robot in people's minds may raise risks towards the right to data protection. Obviously, more uncanny valley increases the trust of people towards robots which, in the end, causes more data disclosure, as will be discussed below.

[348] Mori, 1970 (in Japanese), translated version is available: MacDorman, K.F and Kageki, N. (2012). The Uncanny Valley: The Original Essay by Masahiro Mori, IEEE Spectrum, available here: https://spectrum.ieee.org/automaton/robotics/humanoids/the-uncanny-valley Last accessed: 8 August 2020.
[349] Darling, 2017, n. p. (preliminary draft)
[350] Richert et. al., 2018, p.420.

Privacy is not a specific issue with robots since problems related to privacy and the use of technology already are on the table with the existed technologies[351] which we also do believe so. However, what makes the social robots specific in terms of data processing is the risk of "false polarization between human-human and human-robot interactions" which is a result of "verbal, empathic and linguistic responsiveness" leading people to share emotions, opinions, views, in short, any personal information[352]. Interacting with a robot by placing emotions, on the other hand, might be a precondition of receiving more personal services. It is all true, that a social robot should know more and more about the person who is being served, make empathy with him and understand him completely in terms of human needs[353]. In this one-way relationship, it is the human who falsely perceives a robot as a human[354] in which, as a result, cause human to disclose any personal issues with a machine. Anthropomorphized machines just encourage people to share more by making them forget the fact that what is shared is recorded and processed by the machines.

HRI and friendship-alike relationships between human and a robot might be one of the preconditions for people to raise the quality of their life[355]. Graaf highlights several aspects of human-robot relationships, by stating that, "robots embedded with sociable interaction features, such as familiar human-like gestures or facial expressions in their designs, are likely to further encourage people to interact socially with those robots in a fundamentally unique way"[356]. However, we do not yet know the frontiers of this unique relationship. Robots engage people with their social cues, as it happens yet only between humans.

Emerging researches in the field of robotics show that not only HRI but RRI is also possible and might even be demanded by the industry[357]. In this way, a robot could learn from a robot e.g. to recognize an object or to adapt the user's personality. This case particularly raises a question on the limit of robotic interaction with each other and share personal data. As a result, more uncontrolled way of data processing should be expected, but we exclude RRI since we focus on human as a data subject (robot as a data subject might be an idea for far future, but the work which discusses robot consent[358] shows that there are researches who

[351] Bisconti Lucidi and Nardi, 2018, p. 6.
[352] Ibid., p. 18.
[353] Fosch-Villaronga, 2017, p. 254.
[354] Bisconti Lucidi and Nardi, p. 20.
[355] de Graaf, p. 590.
[356] Ibid., p. 592.
[357] Google, Methods and systems for robot personality development, p. 13.
[358] Frank and Nyholm, 2017.

thinks about the far future from now). Before becoming *homo informaticus*[359], people interacting robots are data subjects whose rights and freedoms should be ensured in an integrated way in the frame of the EU's data protection law.

The last observation we made during this research is regarding the possible emotional bound a vulnerable group may establish with a robot, leading them to disclose information about their vulnerability. It is expected that there would be more people aged 60 or more, than people aged between 10 and 24 by 2050 in the world. Eldercare, in parallel with this fact, maybe of the greatest importance for the young population who is also the work-force within the society. Leaving the cultural and ethical issues aside, social robots could play an important role to balance elder care and would be the catalyzer of the non-disrupted workforce because of this reason. Social robots could eliminate discrimination against elders which happens because of a lack of resources in general, and ensure that they get the proper care. Indeed, elders want to live an independent life with the help of robots who could manage their daily needs at home. However, as the research shows, they concern about their data protection and privacy rights most[360]. These groups indeed need particular attention when designing robots specifically to serve them based on their vulnerability (will also be analyzed in detail in Section 2).

1.3. Social Robots and the GDPR

In the previous paragraphs, we explained how AI in general and a social robot in specific could drain big amounts and different types of personal data to make meaningful outputs. In line with the GDPR's related Article 22 referring to ADM and profiling, data processing activities and the outputs based on these actives may raise some further infringements on data subjects' (who might either be the main users or only other people interacting with robots) rights. We will first analyze the risks, then further refer to general issues arising based on profiling and ADM.

[359] Trimmel, 2017, p. 1. Trimmel uses the term for conceptualizing the future's human-robot integration in possible several ways, such as human acting as a computer subsystem, but the concept involves also some current facts appearing as a result of human-robot interaction. Developing an altered social interaction and carrying a risk of problematic technology usage or even technology addiction, together with having some technology competences are some of the indications for being as homo informaticus.

[360] Zimmermann, Ableitner and Strobbe, 2017, p.452.

1.3.1. Profiling

“Big data, machine learning and artificial intelligence (AI) are enabling profitable commercial opportunities and social benefits through profiling and automated decisions”[361]

Under the Article 4 (4) of the GDPR, profiling means “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements”. While the definition highlights the processing and use of personal data to deliver personal services, it is essential to make the connection between the definition of profiling and social robots.

In principle, profiling should be targeting a natural person, according to the definition. Personal social robots at household use cannot be imagined without data gathered via profiling a natural person to deliver personal services, as indicated several times before. Robots should be able to understand the complexity of humans by categorizing their several different behaviors and needs, even at the most sensitive level. The use of profiling appears as it could generate information about people’s personality, attributes, behaviors, interests, or identity, and in scoring or ranking these elements to assist decision-makers[362] or generate outputs specific to the data subjects using robots at households.

The consequences of robot profiling may be unexpected and might exceed the original purposes indicated for delivering the necessary services or assistance to the users. For example, an algorithm may generate such an output discovering the data subjects’ vulnerabilities even they do not know about it. Based on the new information extracted from profiling, a social robot could act itself, out of the knowledge of the users which is sometimes in a positive, but sometimes in a dangerous way. A robot being operated at a household could help the users in emergency cases by transferring an SOS message to a hospital’s emergency department based on their profile and the actual measures at hand (e.g., the inputs: low or blood pressure, slow inhalation; the output: medical assistance is needed) together with their medical history. Such a service could save the lives of users or other participants living in the household, but at the same time, result in a transfer of a medical history of the data

[361] ITU, 2018, p. 16.

[362] “Data Is Power: Profiling and Automated Decision-Making in GDPR”, [Online], Privacy International, 2017 Accessible from: https://privacyinternational.org/sites/default/files/2018-04 Last accessed: 10 January 2020.

subject to the hospital. Further, we could refer to the several ML techniques that were described previously. Most of the AI services are being evolved with real-time data today, making the use of past data less observable. Profiling contributes and develops this living organism by entrusting real-time personal data flow. More living data brings more new decisions that could change the main purposes of the algorithm. One of the consequences of constant profiling may be losing the original legal bases that the data controller referred to at the beginning of data processing, later without realizing it. For example, consent-based data processing activities may be invalid or become unfair, for future data processing activities that are strictly related to the core purposes since they may differ by the time drastically. The below further analyses will serve the purpose of illustrating this statement.

1.3.2. Automated decision-making

Article 22 of the GDPR entrusts data subjects the "right to not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" unless such a decision is legally permitted or is a result of action based on legal permission such as explicit consent.

First of all, it should be argued what is an ADM, the considered legal effects, the significance of the decision, and whether Article 22 applies to cases where HSR operates in private spheres. To begin with, there is no doubt that AI is initially an ADM procedure from the aspect that it processes data totally in an automated meaning without any or few human influence to the result of the processing. The automated recommendation systems, such as Google's search engine optimization tools or Instagram's content recommendation tools are examples of the ADM tools. According to the Article 29 WP, unless a human involves the processing of the final decision about the data subject, the decision is counted as it was made based solely on the ADM tools[363]. An HSR developed with an unsupervised learning technique such as the RL, and moving around a household collecting and processing personal data (which actually is referring to the term profiling) without any interpretation by a human on the collection and the results of data processing surely operate in an automatic meaning. Secondly, as mentioned before, social robots involve very personal life of data subjects, such as they could analyze their emotions, or be placed in their homes to support their health conditions, or just to entertain them. Taking the example of a robot designed for supporting the data subjects' health condition, the outcome (the decision) which the robot

[363] P20

produces about the health status of the data subject would indeed significantly affect the data subject. For example, if the data subject's health condition is elaborated as under depression by the robot which also assists the user to order her ordinary medicines, the robot may decide to order some non-chemical medicine to fight against depression (in case the user already consented for such an action before). This brings a degree of data disclosure to the pharmacy or the others seeing the content of the order box. Furthermore, the robot may wrongfully evaluate the health condition of the data subject causing money loss on the non-chemical medicine (or causing damage to the health of the data subject, in an extreme case). The individual might be refused to access some of the basic job opportunities because of his health condition. On the other hand, an HSR may track the other people at home expanding the profiling and ADM process. Algorithmic assessments based on profiling of third parties may also cause a breach of rights of other people which, in our opinion, is a clear significant legal effect. More insight about the ADM and the significany of the algorithmic decisions will be presented in the Algorithmic Decisions Affecting the Data Subjects part.

Finally, while the HSRs involve the personal issues of the data subjects, the data they collect, and the process, is the most sensitive data/data belong to special data categories. Referring to the special categories of personal data is important in this sense because the risk of breach of fundamental rights raises whenever sensitive data is evaluated under the ADM rules. As a result, the applicability of the Art.22 of the GDPR on HSRs without a doubt is valid, since the HSRs are systems conducting ADM procedures on personal data without human intervention and could easily generate legal effects on the data subjects.

The prohibition of ADM is not valid if one of the conditions listed in the Art.22 (2) of the GDPR is met. These conditions are, namely, if data processing through ADM is: necessary for entering into, or performance of, a contract between the data subject and the data controller; permitted by law; and based on data subject's explicit consent. In cases where ADM is permissible (specifically through consent and explicit consent), the data controller should ensure data subjects' right to request human intervention, to raise an objection, and to express their own opinion related to the decision. For the decisions made through a processing activity based on a single or several special categories of personal data (such as data related to health, or biometric data), the data controller must effort better safeguarding data subjects' rights and freedoms. Recital 71 of the GDPR states that data subjects have a right not to be subject to decisions made or the measures taken significantly affect them and as a result of the solely automatic data processing activity. Such decisions are already made often in our daily lives without feeling its significance or without having a chance to evaluate whether they significantly affect us.

Let us take the example of marketing messages delivered by social media tools in a variety of ways almost every day and displayed on our devices. Facebook ads, for example, are displayed as a result of ADM procedures taken to deliver tailor-made advertisements based on our search history, private messages (through its Messenger service). Facebook services should not normally include political messages to manipulate people's choices but the success of Brexit and Trump administration is based on profiling and ADM. Without profiling people and generate persuasive messages to the targeted voters (although none of them was consented for delivering such messages) both of them would not have occurred. No human practically involved, control or monitor what and how Facebook's algorithm decided to place a personal ad on people's screens. Even in this case, Article 22 is still fully applicable even though no one truly could prove the significant (and legal) consequences of Trump's election and the advertisements on the individuals' life.

Some of the other examples when the decision was made by an algorithm creating a significant legal effect will be the last discussion under this title. The example also shows the problematic nature of correcting the output of an algorithm. Last year, the Swedish Public Employment Service denied some of 70 thousand unemployed people to access government benefits, cost around 75 million Euro[364]. The decision was based on an algorithm checking the beneficiaries' status whether they fulfill their obligations (via activity reports) and other indicators such as their financial status. However, the algorithm generated the so-called false positive/false negative outputs that affected individuals' access to the benefits. While the authority has promised to correct this mistake, it took a year for the authority to realize this mistake which came out as a result of a technical check upon dysfunction of the system to execute its routine services. If the system was functioning well for a long time and if technicians did not realize the problem, people's financial loss would be even bigger. These are significant issues, however, their existence is hardly provable.

Article 22 of the GDPR includes two different terms that are associated with each other by the EU legislator: ADM and profiling. Profiling, as mentioned before is unavoidable when an HSR operates either at households or public spaces. However, what about profiling other

[364] "Sweden: Rogue algorithm stops welfare payments for up to 70,000 unemployed", [Online], Tom Wills, Algorithm Watch, 25 February 2019 Accessed from: https://algorithmwatch.org/en/rogue-algorithm-in-sweden-stops-welfare-payments/ Last accessed: 27 February 2019.

people (third party natural persons) that are not the initial users of the HSR and further without their consent?

1.3.3. Profiling and ADM: The Potential Data Subjects

The GDPR safeguards data subjects' right not to be subject to such automated decision-making procedures and profiling, in Article 22 as described before. Either the main user or the other people entitled to robot profiling should be ensured to choose between being under robot surveillance or not, the rule is fully operable.

We simply claim that HSRs at personal use would not only observe the main user's data, but also others' data around the user, e.g., family members and friends. Tucker calls this issue the "group privacy problem"[365], that we specifically analyzed in this work from the aspect of consent and informing obligations. Basically, an HSR would first be profiling its main user but profiling others at the households is unavoidable. On one hand, such comprehensive profiling could be necessary to better serve the users and might even be demanded. On the other hand, the data spillover effect may interfere with other people's right to data protection. For example, other people's picture and voice data might be collected during the HRI and might be processed firstly for a significant purpose. However, as a result of constant interaction which leads the robot to collect more information about the others, different outputs may be reached based on the processing of a bigger amount of data. Another example given by Tucker refers to the ML techniques unintentional but successful in finding the relationship between people with the same or similar categories based only on their genetic data, therefore causing a data spillover effect. Similarly, an AI can use any digital data retrospectively even though the data subject does not remember the reason for its creation, and processing activity may cause disclosure of data of persons other than the main data subjects[366]. For example, a picture of a user with her friends published a year ago on Facebook might be processed, and be combined with another data disclosing the friendship (even the level of the relationship) between each other.

Besides the ML techniques, robot personalization (which occurs on an ongoing basis) could also contribute to raising these. For example, a robot could access the user's e-mails, text messages, or calendars to understand the user better. It could easily find out what kind of and how much deep relationship does the user has with particular groups of people (family,

[365] Tucker, 2019, p. 427.
[366] Ibid., p. 430.

friends, professional network, etc.). To analyze this relationship, the robot must examine others' profiles and place them within groups. Such a problem has never been addressed by any of the EU documents yet. We also adopt the data spillover effect and reflected its consequences in the scenario.

Furthermore, personal data could be processed for another purpose than it was originally collected, because it can discover correlations between the data at hand. For example, an AI algorithm that could successfully guess the data subjects' sexual preferences from their pictures on a dating website[367] could show how data about a user could be generated out of his knowledge and also for another purpose than the original purpose. Those who were subject to this work surely did not publish their data on a dating website for their sexual preferences to be identified. Such processing activity is referred in the literature with the term purpose creep that will be later discussed.

Finally, what if a social robot at a household would interact with other persons around the main user, and intentionally disclose information about each other? Intentional data disclosure by a robot was tested by Syrdal et al[368] who proved such a possibility based on the experiment they carried out. The experiment was based on a scenario, in which a robot was placed between two people having a conversation about their daily life issues. During their conversation, the robot reveals information about the experimenter's (the user) sleeping and cleaning routine which were evaluated by the participants acting quite disturbing. An HSR, in a similar way, could reveal information about its user's health condition to other people without her will. Such interferences raised by the machines that are not protected by the GDPR will be the focus of this research and the scenario presented directly refers to the question.

The examples we have given during the evaluation of ADM and profiling made us question an important aspect of the GDPR, we believe, that is the core principles of transparency and purpose limitation. We raise the following question: How human could exercise her right not to be a part of an automated decision-making system ex-ante (so before seeing whether the decision would have some significant effect or not) when the algorithm already made the decision? Even if the last decision is given by a human, it was stated that it is either not

[367] "Artificial Intelligence Can Identify Gay Faces from a Picture, Study Claims", [Online], Aatif Suleyman, 2017, The Independent. Accessible from: http://www.independent.co.uk/life-style/gadgets-and-tech/news/ai-gay-faces-facial-recognition-study-claims-artificial-intelligence-a7936851.html. Last accessed: 11 November 2018.

[368] Syrdal, et. al., 2007, pp. 28-33.

possible or not clear how human intervention could be legally described.[369] Let us present the decisions possibly reached by the machines and the significance as well as possibility of human intervention to those decisions.

1.3.4. Algorithmic Decisions Affecting the Data Subjects

Finding out the legal significance of the output generated by algorithms based on profiling could be explained by the taxonomy of algorithms. For that purpose, we referred to Van Otterlo's taxonomies consist of two main groups. He borrows the first taxonomy from Mittelstadt et.al.[370] who referred to the main operations of the algorithms turning data into a persuasion tool, to make people rely on algorithms' outputs, therefore making decisions. Once a decision-maker made a decision based on this output, an act is born, so algorithms become the main reason behind the human decision. As we referred before, AI could also execute its own decision, but human decision making based on algorithmic evaluations has yet more existed in practice. Algorithms simply make some statistical analyses to generate some significant results. These decisions may not always be the ones the data subjects would like to hear or share with the others. In this case, the decision may have either negative or positive results for a person in-subject, without a possibility to guess priory[371].

The second taxonomy van Otterlo identifies is the level of agency or autonomy which refers to the abilities of the algorithms. These abilities are related to the algorithm's ability to:

- extract information from a large amount of data by profiling from existed resources to reach personalized outputs,
- learn how to create general rules,
- optimize the services to manipulate user behaviors through reinforcement techniques,
- be physically present,
- be superintelligents that are capable of doing everything even better than humans.

Van Otterlo's self-taxonomy points to two of the basic problems that we deal with in this work. Social robots extracting and interpreting personal data together with the reinforcement learning technique, and its physical presence leading them to be human-like actors in real

[369] See, Veale and Edwards, 2018, p. 400.
[370] Mittelstadt et. al., 2016, p. 18.
[371] van Otterlo, 2018, p. 28.

life which raises questions from consent, purpose limitation, transparency, and liability problems. Since we leave out the discussions referring to the possible electronic personality and robots' liabilities, we continue the analysis with the persons (actors) involved with AI technologies and data processing.

1.4 Data Subjects

There is no specific definition the GDPR refers to describing the data subjects. However, the definition of personal data (as we also referred before) includes the term data subject and gives a clue on what to be understood from this term. According to that, an identified or identifiable "natural person" forms the concept of the data subject. In line with this statement, one may easily realize that the GDPR protects and gives rights only to natural persons. A natural person using the personal robot at home and the other natural persons interacting with robots indeed fall within the scope of this definition. Companies, public institutions, NGOs, and any other type of legal personality are left out of the scope of the GDPR.

1.5 Data Controllers

Until now, there might have been an impression this work has given as the robots are the actors collecting and processing personal data. The GDPR defines the data controllers as "natural or legal person, public authority, agency or another body who alone or jointly with others, determines the purposes and means of the processing of personal data" leaving no room for robots to be evaluated as data controllers. In this case, it is clear to state that only the natural and legal persons could initiate the necessary datasets for the algorithms together with their structures (not robots, indeed, and yet).

Since the definition referred in the GDPR is very broad ("any" natural or legal person could be data controller without defining the level of the degree of controllership) and it remained unchanged as the Directive 95/46/EC, Article 29 WP's explanation on the concept of controller and processor [372]shall guide finding the degree of controllership. The opinion document makes word-by-word analysis, but we would focus only on the "determination of processes and means of the processing" part as used in the definition.

[372] Since the GDPR entered into force, the opinion was not updated although several Article 29 WP opinions were updated in line with it (e.g. EDPS, 2019).

According to WP's opinion, there are three categories of controllers deriving from the purposes of data processing. The first category refers to the controlling activities based on national or EU law, meaning that controlling activity directly is ordered by law. We could say that data controllers fulfill their legal obligations by processing data in line with the law. The second category refers to the controller's processing activities that are not explicitly and directly referred to in law, but still could be established under a specific legal field such as labor law. The last category refers to the factual influence principle in which the controllers do not share the same degree of responsibility. Joint controllership, as we will discuss below, belongs to this category. Additionally, most of the natural persons using personal devices highly likely to be in this category[373]. Finally, predictability plays a crucial role in finding out the controller or possible controllers. Recent CJEU cases[374] concluded on the joint controllership requests by also referring to the predictability concept.

The opinion statement of the WP offers a practical guideline to follow in defining the factual elements in case finding out the means of procession within the specific circumstances. For example, by asking "who determines the processing operations, why is processing taking place, who initiated the processing" could help to adopt a pragmatic approach to identify the controller. Furthermore, it is strictly expressed that deeper analysis is needed with further guidance to answer the "why" and "how" questions. For example, the person is in the capacity of deciding on the data to be processed, to be deleted, or about the storage time could be a data controller by determining the means of processing. However, answering these questions is not always easy if we compare the cases where there is a clear legal relationship between the legal persons and cases where a natural person facilitates the main controller to reach the main purposes for data processing. Furthermore, the technical fundamentals of AI systems may complicate a clear set of finding the data controllers.

1.5.1 Data Controllers and HSR

There might be several data controllers responsible for the data processing activities of social robots. Developers, manufacturers, users, or any other persons contributing to the social robot's processing activity might be the potential data controller (or processors, depending on a case). However, identifying each controllers' certain responsibilities might be a

[373] In our point of view, Article 29 WP's following opinion is placed in the guideline to point out the natural persons' responsibility in frame of factual relationship: "(this category refers to those actors) making use of new information technologies, where relevant actors are often inclined to see themselves as "facilitators".

[374] Those cases will be analyzed deeply in the following sections.

challenging issue, firstly, based on the technical settings of the algorithms. It may not always be possible, for instance, for the developers to ensure the decision made by a social robot is a bias-free decision.[375] There are many technical reasons for that and these reasons initially complicate the possible liability scenarios. Training data might already include many racist inputs at the time of acquisition and this may lead the algorithm to reach racist predictions[376]. Underrepresented groups may suffer from the biased decisions made by human-assisted by an algorithm[377]. The risk of overrepresentation in the training set as Katyal indicates, in the case of deploying algorithm for crime prediction trained with past criminal data, there is a high possibility for people who has some common features with training data to be labeled as potential criminals[378].

However, as Lehr and Ohm suggest that, focusing only on the running model which raises the main concern on bias issues would restrict the legal researches to discover other important problems such as the problems arising from playing with the data at the early data collection phase[379]. They identify discrimination as one of the top topics discussed by the legal scholars especially as it is a problematic aspect of ML[380]. The authors gently criticize those legal scholars who argue about the discriminatory algorithms by pointing the possible technical solutions, so that indicating the fact that those worries actually could be intervened easily by implementing technical solutions. Suresh and Guttag[381] draw the attention to the common rhetoric, in their words, that the term bias refers to a harmful property of the data, but in fact, the data is generated in a combination of several factors which may form a degree of error already. To their view, it is not only the data that creates bias, but it may also occur during labeling the data, and this could be mitigated by technical safeguards. Our position regarding bias and discrimination, which are the recent topics discussed by the legal academia, is similar to those, that since bias mainly causes harm to the service providers

[375] There are several types of bias in ADM. Yu and Ali refer to two types of bias, namely (i) Algorithmic bias, appearing as a result of algorithms to simulate humans and their values (ii) Data bias, the AI adopts the algorithmic bias and repeats it constantly. A solution would be to delete the data, but identifying and deleting the data from all variables may deprive the AI of the necessary operating information, therefore reaching accurate results. See, Yu and Alì, 2019, p..4-6.

[376] Sandvig, et. al., p. 4979.

[377] Goodman and Flaxman, 2017, p. 53.

[378] Katyal, 2019, p. 75.

[379] Lehr and Ohm, 2017, p.658.

[380] They also referred to explainability problem, as well as accuracy problem, as some of the other most discussed topics by the legal scholars and accept the fact that even the technical solutions may not satisfy the legal requirements or in areas where explainability is at the utmost importance, they suggest that the ML techniques restring the explainability should not be implemented. Ibid., p. 716.

[381] Suresh and Guttag, 2020, n.p.

(loss of reputation, number of consumers, time for development, investment, etc.)[382] they would soon find some technical solutions. The problem with a biased algorithm could be if it is intentionally created which we do not think would be the case for businesses aiming to profit from algorithms. That is why we think that soon there will be solutions[383] for bias even if it would come with some level of cost regarding the accuracy[384].

Specific to this work, we focus on the future direction raised in academia and industry on using dynamic training sets teaching AI how to learn[385]. On one hand, a social robot learning directly from its user could reach more accurate results about the user's personality[386]. On the other hand, it could make predictions not only about the main user but on the other people sharing the household. Since RL techniques show the way to deal with dynamic data, algorithmic decision making based on such data raises concerns on balancing the right to data protection and the possible benefits people may earn from personal robots. Autonomous systems could learn from the direct interaction with the user and constantly design their decision-making system based on the user's inputs. In this case, even the developer cannot know how the system "pick, study and consider variables out of a massive pool of data"[387]. Especially, when the user even indirectly and de facto defines the purposes (the reason "why") influencing some degree of determining the purposes and means and contributing to start for the robots to process data, consequences of using the robot could lead the users to be one of the first addressees for holding liability. Evidently, there are many data controllers as well as data subjects involving the operation of HSRs.

1.6. Joint Controllers

Joint controllership introduced in Article 26 of the GPDR is another remarkable novelty that we could note (recalling some of those novelties from Part II, point 4) before. Joint controllership already existed in the Directive 95/46/EC, but the GDPR brought further rules and explanations on the concept. The main reason why for providing a deeper insight into the concept is the involvement of technologies (web-based services, social media, personal

[382] ITU, p. 36.

[383] There are already several works done proposing technical, but also legal solutions for bias, see, Carmichael, Stalla-Bourdillon and Staab, 2016. Enhancing data protection rights by legally ordering data controllers to take extra steps during and after data mining such as conducting data mining impact assessment, adopting greater transparency tools, ensuring organizational knowledge about algorithmic discrimination.

[384] Grimmelmann and Westreich, 2017, p. 158.

[385] Mikolov, Joulin and Baroni, 2019, p. 36.

[386] Youyou, Kosinski, and Stillwell, 2015, p.1038.

[387] Packin and Lev-Aretz, 2018, p. 5.

health applications, etc.) paving the way for anyone being able to contribute to the main purposes for data processing in certain services.

Article 29 WP delivered most of the interpretations on the concept and notion of joint controllership, again, in an opinion document. According to that, a person who has a chance or right to determine those purposes and means of processing operations together with the controller is a joint controller[388]. Remarkably, triggering the processing activity also falls within the scope of joint controllership. Both recent and previous CJEU decisions approve that statement. For example, whether an administrator of a fan page established on Facebook would be data controller was questioned before the CJEU recently, and the CJEU held the position that the fan page administrator who gave a chance to Facebook to reach those purposes by triggering the data subjects to visit the fan page, is a joint controller[389]. Basically, since the fan page administrator gains benefit from the fan page (such as learning about the audiences to deliver them better advertisement) and assists Facebook to reach its main data processing purposes (e.g., contributing statistical assessment of Facebook's algorithm), they are a joint controller without a question.

The use of such technologies for personal purposes rather than business activity does not exclude such a rule from the application to the natural persons, even if it is not in the same degree as legal persons. Recently adopted EDPS guidelines on the concepts of the controller, processor and joint controllership under Regulation adds further guidance on determining the joint controllers. For example, the EDPS summarizes the joint controllership concept with the following words "(when) a general level of complementarity and unity of purpose could already trigger of the processing operation are jointly determined"[390] where neither of the parties involved in the processing operations would be able to achieve the purpose independently. This statement may qualify a natural person to have some degree of joint controllership since a user of a social robot cannot fulfill the purposes without sharing data. There is no difference between a user uploading (own and/or others') data on social media platforms and a robot user, in this case, although it might be purely for personal purposes. Regarding this topic, two specific cases interpreted by the CJEU, namely, Lindqvist, and Ryneš cases will be later analyzed to explain our statement.

[388] Article 29 WP_1/2010, p. 18.

[389] Although Facebook also is a data controller, since it decides about the processing purposes and process data via cookies. Case C-40/17 Fashion ID, para. 75.

[390] EDPS, 2019, p. 23.

Possibility of natural persons to have joint controllership eliminates the so-called household exemption and makes them responsible for the use of personal data (of others) for their cases, even though we are conscious about the narrow interpretation of the household exemption and data controllership of the natural persons. Case by case analysis is needed for such cases when natural persons use a social robot for their personal purposes, but paving the way for a social robot to profiling other persons. WP's opinion, and the GDPR, support this view together with a note referring to the indisputable obligations and duties of main data controllers (e.g. Facebook, Google, social robot's creators) which do not change their main data controller role. Duties, obligations, and responsibilities of joint controllers as natural persons should be clearly defined for avoiding possible conflicts on assigning liability to the actors. For example, a clear interpretation of the household exemption could help users to feel more comfortable leaving no risk for them to be held liable while using an HSR. On the other hand, possible scenarios that may cause users to be called joint controllers also should be communicated to the users.

1.7. Data Processor

Data controllers and joint controllers are not the only actors involving data processing activities. Indeed, there might be fewer data controllers and joint controllers than data processors in today's connected world. Data processors are natural and legal persons (separate then the data controller) acting on behalf of the controller for specific data processing activities assigned them by data controllers. Their roles are assigned by the data controller, at least, in terms of identifying the purposes and the means of data processing activities. As long as they act in the frame of data controllers' instructions, they are the data processors, however, they may be both data controller and processor at the same time, if they create new data processing purposes for the data they process for data controllers. During our research, we realized the fact that involving data processors in the scenario would make the present work's analysis part extremely complicated. Therefore, we leave out the actors that may qualify as a data processor for presenting a smooth analysis.

Section 2. Practical Problems

This section concentrates on the practical problems arising from the personal use of social robots at households from the data protection point of view. A variety of questions were raised during our research, such as, whether the household exemption would apply to the household social robots. Some of the core principles of the GDPR, which are also subject to the analysis of this dissertation, such the consent, purpose limitation, and transparency principles will be discussed. The following descriptive analysis will show the main reasons for this statement. We believe that the AI's technical complexity, combined with data controllers' possible justifications to avoid legal responsibilities, and practical issues arising from the application of the GDPR on AI technologies complicate the applicability of the rules, principles, and rights assigned to the data subjects in the GDPR. The question "who is liable" is almost unavoidable in any AI-law related work; in this case, we also place this question within the analysis, but our intention is not to give a concrete answer to this question, rather we focus on the possible answers. Further, expert interviews will be analyzed and solutions will be presented to provide proactive solutions.

2.1. Legal Bases for Household Social Robots Processing Personal Data

Which legal bases could be referred by the data controllers for operating social robots processing personal data? What might be the eligible legal bases enabling social robots to process data and reach predictions?

One of the principles of processing[391] personal data is the principle of lawfulness placed under Article 6 of the GDPR. GDPR offers many options for data controllers operating social robots to choose a concrete legal basis for the robot's data processing activities. Article 6 paragraph 1 of the GDPR refers to the following legal bases to the data controllers to ensure legal data processing if the processing activity is:

- necessary for the performance of a contract,
- necessary to the data controller to comply with its legal obligation,
- necessary to protect the vital interests of the data subject or another natural person,

[391] Processing activity here means as the Art.4 of the GDPR indicates: any operation [s]uch as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In short, processing covers any activity related to personal data.

- processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller,
- processing is necessary for the legitimate interests pursued by the controller or by a third party.
- based on data subject's consent,

Following, we would evaluate these legal bases specific to operating a social robot for personal use at home.

2.1.1 The right legal basis for HSR

Finding the right legal basis for operating social robots for personal use could be illustrated via an example from our everyday interactions with technology. Consider the following personal mobile phone use case: an application embedded in a certain type of mobile phone comes with the phone by default, and is an essential part of the phone (for example, the mobile phone's operating system). If the components of the application which are essential to make the phone work require personal data processing, then the legal basis for such data processing would be most probably based on the performance of a contract. However, as the Article 29 WP explains, "building a profile of the user's tastes and lifestyle choices based on his click-stream on a website" cannot be considered for the performance of a contract rule since this is not necessary for offering the main service (e.g. delivery of the service)[392]. Valid contracts can only justify those data processing activities written in the contract[393], no more or no less than what is written there, limiting the data controller's space to gain profit from the data at hand. On the other hand, the performance of a contract rule is applicable only if the reasons for data processing activities are same as the reasons entering into a contractual relationship with the data subject (indeed, there can be a contractual relationship between two legal persons, but we exclude that probability, for now). Data processing activities operated through personal mobile phones are generally neither connected to fulfilling data controllers' legal obligation nor processing for the necessity of protecting the vital interest of any person (exceptions excluded). Further, when somebody uses a mobile phone, legal persons behind the mobile phone, e.g. manufacturers, or software developers, do not process data to execute some tasks related to their public interest, generally. Data processing for performing a task carried out in the public interest does not apply unless the

[392] Article 29 WP_06/2014, p.16
[393] Voigt and von dem Bussche, 2017, p. 242.

mobile phone is not a part of public service. In this case, few options are available for data controllers to operate an HSR: the legitimate interest rule or consent.

2.1.2. Legitimate interest rule

Legitimate interest is another legal bases that could be preferred by the data controllers to process personal data. There are several conditions for choosing legitimate interest rule as a legal basis, based on the examples referred in Recital 47 of the GDPR: if there is a relevant and proportionate relationship between the data subject and controller, the data processing activity is expectable by the data subject from the time and context aspects, processing shall be identified as raising low risk towards data subjects' fundamental rights (might be identified based on the DPIA), and the data subject is a client or at the service of the data controller. Processing personal data for direct marketing purposes might be an example of such an interest. Commercial interests, societal benefits, interests of third parties are also to be considered as the legitimate interest of data controllers[394]. Another most common example of legitimate interest rule is the CCTV cameras in which data subjects have no option to opt-in or out, due to the data controllers' legitimate interest which is very specific (security). Clearly, legitimate interest is needed if the processing activity is at the benefit or interest of the data controller, not for the data subject. Interests do not tell us the reason why for data processing activity, for example, if the data subject is the beneficiary/receiving party of the services (e.g., using the robot for ordering food) then legitimate interest cannot be applied[395].

Data processing based on consent, on the other hand, is different from the legitimate basis rule since the data subjects themselves authorize or allow the processing activity where legitimate interest refers to for data controllers' interest. However, there is a relationship between legitimate interest and consent rules. Even if no consent is needed before the processing activity based on a legitimate interest, the data subject must be provided the existence of the interests and relevant information, together with the possibility to stop data processing. Data controllers' informing obligation under the legitimate interest rule is a common future with consent rule.

[394] "Legitimate interests", ICO, [Online]. Accessed from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ Last accessed: 29 October 2019.

[395] Article 29 WP_06/2014, p.24

There is a discussion ongoing regarding whether the GDPR offers any more clear and right legal basis for the data controllers operating AI systems than the legitimate interest and consent. Sartor[396], in his comprehensive analysis specific to the impact of GDPR on AI, states that the legal bases for data processing indicated in the GDPR do not fit on purpose with the data processing in AI, except the consent and legitimate interest rules[397]. For him, there is a necessity to make a difference between using the data as an input to a learning algorithm and using the same data as for evaluation in the learned algorithm. Since the legitimate interest rule goes for the data controllers such as the ones developing an AI system, personal data could be obtained based on a legitimate interest rule to be used as training data. However, as clearly reflected before and will be reflected several times throughout this work, personal data submitted to the algorithm for evaluation is not only under the legitimate interest of the data controller but also serves to the interest of the data subject. Sartor's analysis also showed[398], that there is a difference between the training data and the data to be evaluated, in this sense, and both of them could be eligible for personal data. Therefore, for social robots evaluating an individual's aspects, let it be health or psychological status, needs to operate under the consent rule. Anyway, although it is unacceptable, the practices of data controllers today show that they chose to obtain the consent of data subjects since it is easier to obtain, it gives more comprehensive data processing opportunities and it brings less strict obligations for data controllers.

2.1.3. Data processing based on consent

Referring back to the performance of a contract and consent rules, even if the application is essential to operate the mobile phone, it works as following in practice: Once we start using a mobile phone (by entering into sales contract), we immediately find ourselves in pages of consent texts offering a more personalized experience, because none of the application worth using without personal components. For social robots to operate, consent seems like the best choice for a data controller to rely on, because no other legal bases apply to the services that a social robot could offer besides its basics functions. For example, a social robot may interact directly with humans to make them happy or lift their spirits as basic contractual terms, however, for the robot to provide a personalized service to make human feel happy consent appears to be the best option for the data controller. In the scenario, we benefit from

[396] Sartor, 2020b, p. 50.

[397] He also discusses the contractual obligation rule besides, and indicates that processing personal data for entering into contract does not cover the business analytics.

[398] Sartor, 2020b, p.38.

this simulation for such applications making the use of a mobile phone's main operating systems but still independently processing data. However, consent may not always be the best option in terms of safeguarding fundamental rights of the data subjects, since it focuses mainly on the systems in the traditional meaning, not on the autonomous machines.

Consent is a term referred in civil law to express either an agreement between at least two parties or more or an expression of a will related to a certain offer[399]. In Europe and, in a data protection specific framework, consent is being used as an indicator of a will that safeguards freedom of data subjects to control their data and imposes legal obligations to the data controllers. GDPR defines consent in the Article 4 (1) as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her". There are, obviously, certain rules on how data controllers should obtain data subjects' consent, such as, in what cases, in what form, or when the consent should be obtained. Although Directive 95/46/EC and the GDPR are distinct from each other in several ways, the question how consent should be obtained is still quite a similar to each other or with the words of the Advocate General Szpunar, "requirements for giving consent are the same under Directive 95/46/EC and Regulation (EU) 2016/679"[400]. However, there are several problems related to the practical and legal meaning of consent, as we will explain below.

The opinion of the Article 29WP on the definition of consent prepared for Directive 95/46/EC [401] and Guideline on consent prepared under the rules of the GDPR[402] could give some overview of how the consent shall be obtained. According to the WP29, consent should be valid if it is specific, freely given, informed, and indicated with a clear affirmative action or statement to allow the data to be processed. To make it specific, the purpose(s) of the data processing should be clearly defined and the data subjects shall be informed about them by the data controller. GDPR's Article 7 requires consent to be unambiguous or explicit depending on the type of the data and to be indicated by an affirmative action (known as the opt-in rule). There are two types of consent indicated in the GDPR: consent and explicit consent which the difference is clear as the type of personal data determines. For example,

[399] Le Me´tayer and Monteleone, 2009, p. 139.

[400] Opinion of Advocate Szpunar, para. 3.

[401] Article 29 WP_15/2011.

[402] Article 29 WP 2016/679.

processing biometric data which is sensitive data is possible if the data subject gave explicit consent according to Article 9 of the GDPR.

If obtaining consent requires a clear purpose statement, could a data controller of social robots put all related aspects of the use of personal data and the future of such data? For example, Big Data and ML techniques naturally could turn “normal” personal data into “special” personal data easily[403] which would not be clear for the data controller to make a specific indication before data processing. Even if the data subject gave consent before the data processing started, it may not always easily be foreseeable what other purposes could algorithm conclude the outcome for. Moreover, neither the developer nor the service provider could foresee the extensions of the scope of the purposes. People (without their and even the system engineer’s prior knowledge) may unexpectedly be classified in a certain ethnic group based on their skin color[404] when they interact with a robot for another purpose than this one. Using such robots with their unexpected consequences may make users feel uncomfortable living with them. However, the algorithms are operating to know the unknown ones, to predict the unpredictable ones in principle, the unpredictability is already coming as part of the game. Whether the GDPR was designed for unpredictable personal outcomes needs another illustration.

Let us take the detriment rule as an example. The detriment rule refers to the possibility for data subjects to keep receiving the services even after revoking their consent without an additional cost or a clear disadvantage. In the EDPB guidelines where detriment rule is introduced[405], one may easily realize that all the examples shown are related to personalized vs. impersonalized services which are clearly distinctive in case of AI-related services. Since the algorithms are for evaluating the personal aspects of individuals, e.g., one’s eligibility for a certain job vacation or bank credit, it is not easy to imagine algorithms to generate impersonalized scores. Detriment rule seems not an easy element to comply with as part of the consent rule.

The consent mechanism was constructed to give data subjects a possibility to choose what data they would like to share with others and to control those shared data, and in other cases be able to exercise their rights if damage occurs. In this case, we could claim that consent

[403] Veale, Binns, Edwards, 2018, p. 2.

[404] “IBM Used NYPD Surveillance Footage to Develop Technology that Lets Police Search by Skin Color”, George Joseph and Kenneth Lipp, [Online], The Intercept. Accessed from: https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/ Last accessed: 10 October 2019.

[405] EDPB, 2020a, paras. 49-54.

gives data subjects the steer for controlling their data. However, when data subjects are not in a sense of the value of their data, or not willing to manage it because of complex procedures, or do not have time to do it, or not aware of the risks of not doing it, consent becomes meaningless. Further, there is another possibility which is the technologic complexities and the data controller intends to present these as an obstacle to fulfill their legal obligations.

The data subjects are expected to be aware of any possible consequences of using such technologies (together with a margin of their technical impossibility) together with the possible risks specific to the technology. The data controller, on the other hand, is responsible to let data subject know about all the possible consequences of data processing. In medical procedures, the informed consent is carried out before a patient receives a treatment (e.g., surgery) and the responsibility for informing the patient about all possible risks, benefits, alternative solutions, and the consequences of the treatment belongs to the doctor who probably would be held liable if fails to fulfill this obligation[406] but who is also the expert who is aware of almost all possible scenarios.

The following analysis, as well as the entire present work, will shed light on the question of whether the concept of consent is a fairytale[407] , especially in case systems. Expecting more than 500 million EU citizens purchasing services from different data controllers belonging to different privacy cultures over the world to always be ex-officio well-aware from a general privacy statement, and then give a perfect consent might be a utopic idea in a practical sense. In the following paragraphs, we adopted a mixed approach for identifying the technical obstacles, possible intended infringements, and identification of specific risks towards the GDPR's full application specific to the consent from the eye of data controllers.

2.2. Unpredictable Robots by Design

Jason Millar and Ian Kerr, the inventors of the term Unpredictable by Design[408] use this expression for the robots constantly acquiring new data, feeding the algorithm with them, and generating such outputs that are almost impossible to foresee from the beginning of the whole processing activity. This statement should not be mixed with the questions regarding

[406] O'Sullivan, et.al., 2019, p.8.

[407] Svantesson, 2015, p. 135-140.

[408] Millar and Kerr (2016) are not the first and only researchers who thought of the unpredictability concept for autonomous machines, but they are focusing more on the technical aspects of the term. See also, Barfield, 2018, p. 198.

the level of robot's autonomy with special regard to decision-making capabilities The term points out the fact that the algorithms receive such a vast amount of inputs, that in the end, the outputs become unpredictable[409]. Leslie, in a later work, calls this unpredictability as brittleness which the term refers more or less the same aspects deriving from implementing ML models especially neural nets on data. According to him, AI systems make unexpected mistakes (outcomes) because, besides working with a big amount of data, they may meet unfamiliar problems to their operation since they may not have the sense to contextualize the problems and are programmed to solve the unknown problems[410]. His approach, as italicized in the previous sentence, is referring to the mistakes generated by the algorithm while operating in the real-world and these mistakes are, naturally, unexplainable due to their computational complexity. On the other hand, there can be unexpected situations where the system may operate well, so not making any mistake, but its actions may not be welcomed by humans. Leslie gives the RL technique as an example where the AI system maximizes its rewards to reach the desired objective but causes harm to people on the other hand. This is mostly because the system is lack of common sense, empathy, context-awareness, and understanding which also cannot be programmed by the developers.[411] In real-life applications, some examples are referring to the unpredictability aspect of the algorithms in a way that their initial creation reason completely changes by time as long as it is fed with new data. For example, Microsoft's racist chatbot which was initially created only for having playful conversations with people turned later out to be (besides making racist statements) foreseeing the reasons behind Trump's idea for building a wall in the Mexican border successfully[412]. So, why algorithms cannot remain working just for the initial reasons for their creation, by time?

Several studies look for answers to this question from different perspectives. For example, Kaori[413] links her answers to two important elements of AI technology: machine learning and deep learning, and the possibility of a general AI[414]. Our statement is in line with their views, but we put more emphasis on the importance of data here.

[409] Millar and Kerr, p.108.

[410] Leslie, 2019, p.30.

[411] Ibid., p.33-34.

[412] "Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day", James Vincent, [Online], The Verge, 24 March 2016 Accessed from: https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist Last accessed: 10 October 2019.

[413] Ishii, 2019, p. 3-4.

[414] Van Otterlo's classification of algorithms and their risks before data protection rules are similar to this approach.

Data is used in the social robot's algorithm could be anything if we recall the previous statements. A robot deployed with DRL would need to access the user's device or profile to get new information about the user and process the data for this purpose. When a social robot receives any information that may cause fundamental changes in the way of algorithm's decision-making system (through ML), which is not predictable by its creators but still is a feature of the AI system, it is the nature of the algorithm itself, not a systemic failure or a bug[415]. In such a way, the technology enabling AI brings these results naturally. The situation is also considered by the EU in one of the official documents as follows: "robots empowered by AI may act in ways that were not envisaged at the time when the system was first put into operation"[416]. Unpredictable by design is a conflicting fact almost with all principles of legal data processing. Because if an algorithm is unpredictable by design, then, practically, neither the data being used in decision making is predictable, nor the purposes of the processing of those data are.

Besides the unpredictable outputs generated by AI, we hereby introduce the *unpredictable data collection by design* concept based on the fact that AI systems are expected to collect data in an unexpected form, content, and amount in an indefinite time. Here, the importance of embodiment makes a different overview of the problem. For example, if AI is a software, it is generally not supported with advanced techniques e.g. NLP and moving cameras, it leaves more margin of personal control on personal data. In this case, we once again raise our argument, that social robots are more likely to process more personal data, and controlling the whole data collection and processing procedure is almost impossible. A machine circling in households and interacting with a human would already and expectedly obtain more data about its environment. Moreover, when human interacts with software, it is not real interaction, meaning that it is not always constant and natural as this is the case with a social robot. Relationship with this statement and the consent is that such an AI software may execute certain consent duties through, for example, a pop-up appearing on the screen where human is given time to read, think, and react. However, physically equipped active objects circling in the household borders with certain capabilities of social interaction, such as NLP and natural expressions (uncanny valley effect), would not give the

[415] Millar and Kerr, p. 108. The authors call it a feature of AI, not a bug. This is really a true perspective on evaluating AI technologies. If a human was capable of gaining and draining some zettabytes of data within some seconds, evaluate them, and make decisions, we would not need algorithms. Such discussion should be out of the scope of this work, but our position is that the algorithm's unpredictability is s natural result of a learning machine.

[416] EC, 2018a, p. 5.

same possibility to data subjects to think of giving consent to the social robot. As a result of all data collection capability of a social robot make us name this case as unpredictable data collection by design which makes data controllers reaching a certain treasure list of data they collect (unwillingly). Santoro, Marino, and Tamburrini say that “if a learning (personal) robot were sold in a shop, prospective buyers would like to find in user manuals a statement to the effect that the robot is guaranteed to behave so-and-so if normal operational conditions are fulfilled”[417]. Keeping the normal operational conditions stabile and ensuring robots’ actions in so and so level is impossible. Involving data and making the system process it with millions of parameters and correlations goes beyond human foreseeability and understanding, therefore neither the purposes nor the explanations on particular outputs could easily be delivered[418]. In such a case, is it possible to still enforce the principles of purpose limitation which is in connection with the principle of transparency that are the main elements of valid consent?

2.2.1. Purpose Limitation and Transparency Principles

Obtaining valid consent is strongly related to the principle of purpose limitation and transparency rules. These rules are basics of all data protection legislation we referred to in the first chapter, namely, in the Directive 95/46/EC, Convention 108, and indeed in the GDPR. We do not intend to repeat the previous statements here, but we shall once again remind that consent is valid if it covers all processing activities on specific purposes and is given freely[419]. For data subjects to be able to make a free decision, they should be transparently informed about the future processing of their data, starting from clear data processing purposes. How much easy it could be to identify the possible purposes an AI system would process the data for is a challenging question due to the technical capabilities of intelligent systems. For example, a social robot making person based evaluations to find out how to feed the user’s needs would need a rich knowledge drained from the personal data. This data often would grow by time and in line with the interactions between the user and the robot, as we several times indicated before. Besides the main purposes, specifying the other purposes appearing and deepening on data often comes after data processing. If the

[417] Santoro, Marino and Tamburrini, 2008, p. 308.

[418] Leslie, 2019, p.43.

[419] Recital 32 of the GDPR.

robot is designed to operate multipurpose or general-purpose[420], then data collection will also be multipurpose or for a general-purpose. A robot may collect data for A purpose, but then use it for X purpose, depending on its capability to find connections between the two purposes.[421] As for data controllers, it may not always be easy to foresee all the other possible outcomes serving different purposes. Furthermore, intentional misuse cases may also appear as we will explain with some examples below. In this case, we could state that there are technical and practical issues regarding ensuring the purpose limitation principle which is one of the elements of the principle of transparency.

2.2.2. Purpose Limitation

The initial problem regarding practicing the purpose limitation principle is related to the technical opportunities an algorithm brings to data controllers (using algorithmic evaluations). Data evaluated by algorithms may reveal new attitudes or new information about data subjects, and that might be either willingly or unwillingly discovered. Despite any list a developer or manufacturer could come up for possible purposes, these might not focus on such derivative ones that the AI might come across in the process. Moreover, data controllers practically cannot even present an acceptable list of personal data that they would process, because even a few data may become another new personal data under algorithmic evaluation. The AI would, in theory, be unstoppable in gathering further data to accomplish its goals and in making those mean something in their environment (as we described with unpredictable data collection by design), in the context of this repurposed activity through generating new data. Both cases are contrary to Article 5 of the GDPR requiring the data controller to collect data as "adequate, relevant and limited to what is necessary concerning the purpose" otherwise known as the data minimization rule. However, data controllers may find themselves both in difficult, but also in an advantageous situation caused by creepy purposes[422]. EDPB, in its opinion, calls this phenomenon as a function creep[423] referring to

[420] General purpose robot is not a futuristic idea anymore. There are already several projects running for this purpose and one of them is the Everyday Robot project aiming creating robots able to interact everyday objects around. See: https://x.company/projects/everyday-robots Last accessed: 15 January 2020.

[421] In such cases, data controllers may not even require to obtain a separate consent. Recital 50 of the GDPR refers to further data processing activities in which the consent was specifically obtained for in line with the original purposes compatible to the other possible purposes, no separate consent is needed to be obtained.

[422] Wisman (2013) indicates that the term is not belong to her but to Jentzsch (2007, p. 39.) who uses the term to describe "the tendency to use information for purposes that are unrelated to the original one for which the data was originally collected."

[423] EDPB, 2020a, para. 56.

the gradual change of the initially indicated purposes by time which might be safeguarded with specific consent to avoid such situations.

In practice, data controllers obviously could explain these creepy purposes at least in general terms, and the other possible separate purposes under risk statement (as a result of the DPIA, for example) as long as the technical meanings suffice. However, they also could choose using technical meanings as a justification to escape from the legal requirements[424]. Data controllers may well use the principles of the GDPR to collect additional information that might not fit the essence of data processing[425]. A study measuring almost 18.000 Android apps' behaviors and their potential non-compliance level with their privacy statement identified out serious inconsistencies between the indicated purposes and real-life practices. From the 9050 analyzed data set including the app and its privacy statements, almost half were found potentially inconsistent, while only a small portion of the examined apps (equals to 1.461 apps) were found completely consistent with the privacy policy they stated[426]. We are not sure whether those inconsistencies were even realized by the data controller, and technically speaking, were even estimated. Even if so, the data controller's unawareness for such infringements still could not be justified since the GDPR obliges data controllers to ensure the secure operation of the systems.

Referring to social robots, and whether their acts could be foreseeable or not, data controllers are still obliged to deliver information about their possible data processing activities. This could be named as presenting "the life-cycle of a specific personal data" within the social robot's brain. Any decision automatically reached by the AI system must be explained to the data subjects in line with the principle of transparency.

2.2.3. Transparency

Data processing in a transparent manner is one of the principles of data processing, as the GDPR Article 5 paragraph 1 (a) describes. Article 12 of the GDPR assigns the responsibility to data controllers for processing any personal data transparently. Transparency rule is one of the basic principles for obtaining valid consent and is referred to under the "Rights of the data subject" chapter in the GDPR. In short, the data controllers are obliged to "provide any information [to the data subjects] relating to processing activity in a concise, transparent, intelligible and easily accessible form, using clear and plain language" to fulfill their

[424] Wisman, n. p.
[425] Vitale, et. al., 2017, p. 442.
[426] Zimmeck, et. al., p. 9.

transparency obligations. According to this statement, transparency rule involves informing obligation for data controllers, and information to be presented involves some of the basic principles such as data processing purposes, reasons, risks, and possible threats.

It should be noted that transparency is more general principle in scope than consent, for example, if a data controller deals with personal data to fulfill its legal obligations which the legal basis is other than consent, transparency obligation still needs to be fulfilled by the data controllers. It is also different than providing mere explanations, talking about the specific AI terminology; where transparency is a working principle behind the technical fundamentals of a system (e.g. the source code of the system), explainability refers to actual information on the reason why the code generated such an outcome[427]. However, no data subject would ever be interested in the code or how the AI model was created technically, they would rather be interested in a specific explanation about their specific situation. In his work which constitutes a guideline as a result of a merge of technical, ethical and legal aspects of AI, Leslie suggests designers and implementers of AI what to understand from transparency as it means "to explain to affected stakeholders in everyday language how and why a model performed in a specific context" and "to justify the ethical permissibility, the discriminatory non-harm, and the public trustworthiness" of the system[428]. Similarly, if data processing is necessary as it is ordered by law, data subjects could request an explanation from the data controller regarding this processing activity. According to the GDPR, the data controller is obliged to respect transparency rules especially data processing activities in line with the rules and descriptions stated in the Articles 13-15, Article 22, and Article 34. It is clear from Articles 13-15 of the GDPR refers to the information obligation, a data controller should provide information to data subjects to fulfill general transparency obligations. From the legal point of view, transparency, informing duties, and providing explanations are all related even if it is specifically implemented to AI systems. To obtain (explicit) consent, data controllers are (again) obliged to provide transparent information (besides fulfilling other obligations). Recital 58 and Recital 60 give a framework about what information to be presented to data subjects, such as information on the processing operation and purposes. Besides, data subjects should be informed about the consequences of profiling, and information related to profiling should be presented in an intelligible and meaningful manner (also applicable rule in Article 22). Article 12 and Recital 60 further states that transparency

[427] House of Lords, 2017, p. 95.

[428] Leslie, 2019, p.12.

obligation could be fulfilled if the information is presented "concise, easily accessible and easy to understand" way.

Explanations are also related to the principle of accountability that is in close relationship with transparency. People need explanations to avoid the wrong impact of the decisions and if this does not happen, questioning the accountability of the decision-maker is unavoidable. Letting people know about the possible errors specific to their situation, as well as the advantages, of being under the evaluation of an autonomous system, is an integral part of accountability[429].

In short, data controllers are obliged to provide information to fulfill their transparency obligation (or their duty to explain according to Article 22 of the GDPR) which is one of the preconditions to obtain valid and also explicit consent. Besides, the transparency principle is related to many other rules and principles in the GDPR, such as profiling and ADM, right to explanation, and purpose limitation. We think that users' consciousness and awareness on the specific AI technology deployed in a social robot is the most effective element for them to be able to make a free consent choice, and data controllers must be fully responsible to ensure whether data subjects received and understand the AI system as a whole. As we will present below, the GDPR could refer some of the basic rules on informing obligation clearer and specific to the AI technologies, therefore no room for misinterpretation would be left for data controllers, but no principle is perfect. Transparency also has its own shortcomings appearing during the application. Based on Ananny and Crawford's work[430] where they argue insufficiency of transparency on governing algorithmic systems, a couple of shortcomings could be mentioned here. The main argument in their work is related to the digital life where transparency is not depending only on the historical contexts that are about revealing information but about a continuous circulation of deployment, configuration, resistance on platforms, machine learning, etc., that manage visibility[431] and understanding them, bearing in mind the following shortcomings. In corrupted environments, transparency might be used as a tool for laundry. It can be harmful if the organizations use transparency as a justification tool for their policies that are not compatible with social values. Information overload would be another shortcoming of transparency which is implemented by the actors without knowing the reason why transparency is necessary. On the other hand, revealing less information on the very core of the system logic affecting the fundamental values of the

[429] Finale and Kortz, p.7.
[430] Ananny and Crawford, 2018, p.978-982.
[431] Ibid., p.985.

society has the same shortcomings weight. Transparency has been limited to the technical establishments as such is the black-box nature of the AI systems and in this case, explainability becomes the driven force behind the right operation of AI systems. System designers and engineers often fail to explain the exact reason why an algorithm reached to a certain output. Transparency, as the authors believe, brings a certain amount of burden on the individuals' shoulders as well as the responsible entities. People need to read, understand, and learn the responsible entity's transparency indications while the responsible entity must generate a clear, concise, long-enough, and just related information. Generating such information for the responsible entities and accepting that information by individuals requires a certain amount of research and knowledge. Human behavior and cognitive process in generating and accepting the explanations needs to be examined scientifically first, and then practice during implementation. An example of such an approach is visible in consumer protection where the scholars contribute to the field by conducting researches on understanding consumer behavior. Data protection indeed needs to be examined with a more general approach than the consumer protection, with general topics such as human behavior, but specific to our work, starting from the human behavior towards the unknown technologies could be a good idea.

2.2.4. Informing Obligation

Informing data subjects about possible data processing purposes (besides other basic information) is one of the utmost requirements for data controllers to obtain valid consent. Articles 13, 14, and 15 of the GDPR, as well as Recital 60 of the GDPR, stipulate that data controllers shall present information related to data processing activities to fulfill their informing and transparency obligations. There is no meaningful difference (at least, in the frame of this work) among the information to be provided based on Articles 13, 14, and 15. Article 13 lists the information to be provided where the data have been collected directly from a particular data subject, and Article 14 lists the information to be provided where the data have not been collected directly from a particular data subject. In both cases, there is basic and generic information to be provided to data subjects; such as the identity and contact details of the controller, purposes of the processing, categories of processed data, recipients of the data, and information on the existence of data transfers to third parties. Further, more information should be provided to the data subjects to ensuring transparent and fair data processing. This information is related to the data storage period, the existence of the right to rectification, the right to withdraw consent, the right to complain to a DPA, and the existence of automated decision-making and profiling. Moreover, as the Article 22 of the GDPR explains, data controllers should provide meaningful information (or explanation) about the logic involved in the ADM system, if there exists an automated decision-making system, including profiling.

What constitutes meaningful information, in the frame of Article 22, has been argued in the literature from several points of view. Firstly, Wachter, Mittelstadt, and Floridi[432] argued that the right to be informed within the GDPR is a general ex-post right which would contravene the essence of consent since the explanation could be given after the decision was made. The authors further stressed that the right to explanation should be inserted in the GDPR to make the rule more consistent and clear[433], and while providing an explanation, no black-box should be opened; counterfactuals explaining the "what would have been the output, if the input had a certain value" would serve to this aim. Selbst and Powles[434], on the other hand, strongly emphasized that informing obligation already means the right to explanation, and meaningful information refers here to any information regarding system functionality. Some foresight was made before the GDPR entered into force on evaluating the difficulty of providing explanations in AI systems (from the practical point of view) pointed that the logic of a model and significance of the logic is enough for explaining the data subjects.[435] Explanation, in contrast, is about exposing information in human interpretable information about the logic what the decision-maker, regardless of human or machine, took those particular steps leading that particular decision[436]. The explanation is meaningless if it is provided without a correct type of information which is permitting humans to understand which particular input was determinate on the output (the counterfactuals, with Wachter's words)[437] without necessarily intervening the codes or sources the algorithm considers in its black-box.

[432] The authors basically discussed a possibility of two types of explanations based on time dependence: ex post and ex ante. From those, ex ante explanation could give information only on system functionality, meaning that only a restricted information such as "the logic, significance, envisaged consequences" on ADM could be given to the data subjects. They also noted that this information is a general information not targeting the personal circumstances that a decision could point out.
Wachter, Mittelstadt and Floridi, 2017, p. 78.

[433] Ibid., p. 80.

[434] Selbst and Powles, 2017, p. 233.

[435] "Is there a 'right to explanation' for machine learning in the GDPR?" Andrew Burt, [Online], Privacy Tech, 1 June 2017. Accessed from: https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/ Last accessed: 27 November 2019.

[436] Wachter, et. al., 2017.

[437] Finale and Kortz, 2017, p.3.

Although both views could not easily and clearly be understood neither from the related articles, Recitals and nor from the EDPS/WP29 opinions or guidelines, we think that the GDPR (as a whole, meaning that by evaluating the Articles 13,14,15, and 22 altogether) is practically not clear on what consists the concept of explaining and the information to be provided to data subjects, from the practical point of view. First of all, taking into account specifically the Article 22, explaining is not about opening the black-box or providing technical information about how the system works, but then, what is the context of the explanation and the information to be provided for? It should be providing such explanations to be understood by the user or user groups about either the functionality of the system or through the counterfactuals; if the data subject does not understand the information or the explanation in whatever form or case, the rule, unfortunately, becomes meaningless.

The GDPR, practically, does not oblige data controllers to ensure the understandability of the information they provide, but provide such information that is generic to all data subjects, whereas reasoning and interpreting AI decision making-tools for human may include several aspects[438]. Formal and logical explanations, or the counterfactuals, on AI's basic working principles all may refer to the logic of AI, while how it works and what does a certain action/outcome means processing refers to semantics. Semantics does not mean much for a simple user, and explaining the logic involved in algorithmic processes does not require opening the black-box. Creating a socially meaningful content of the algorithmic outcomes should serve the society's clear understanding of this technology and this should be away from providing any technical or one size fits all type of information or explanation. Finally, the moral justification aspect should be included in the explanations, because they could make the sense of what to consider as right or wrong in one's choices such as choosing to be under the surveillance of a household robot, or not. These aspects altogether are the factors in explaining the decisions and behaviors of AI which helps to justify the impacts of AI on individuals. This is the societal aspect of AI that needs to be examined. Miller[439] examines providing explanations in the AI concept from the social sciences perspective, and shows that preparing information/explanation in the AI context is not that simple as the GDPR writes down with a couple of words (one size fits all) in the legal text. He focuses on the decisions of autonomous systems, both from the pre and post explanations point of view, and distinguishes the explainability and the explanation of the decisions. He takes as an

[438] Leslie, 2019, p.40. Actually, Leslie more likely generates a guideline for the public sector using AI tools, but his analysis and solutions could easily be interconnected with the private sector, too.

[439] Miller, 2019.

example of the human way of generating explanation with a philosophical approach that requires another examination on human psychology, cognitive processes, external factors affecting the explanations and understanding them[440]. All in all, the factors presented, analyzed, and mutated to preparing an explanation for AI systems in Miller's work show the complexity of human in receiving information and understanding the explanations which become more complicated with the integration of AI systems in human life, which distinct from a legal approach as such the GDPR reflects.

Our above earlier made analysis was approved also in Sartor's work focusing specifically on the analysis of Article 22 and Recital 71 of the GDPR. We both came to the similar conclusion by evaluating the Articles 13,14,15 and 22 altogether where Sartor points straightforwardly and only to the application of Article 22 and states that, the article is missing two items: one of them is the provision of providing specific information in explanations (taking into consideration the conditions of the data subject-specific) and the other one is the right to obtain explanation after the decision is reached. [441] While there is no discussion presented about the timing of the explanation throughout this work, ensuring the lack of a rule for providing specific information is significant.

To conclude this title, there are obstacles in providing meaningful explanations and information in case of AI, let it be under the transparency principle or the informing obligations specific to the ADM, the data controllers must be required to provide a full range of information in a way each data subject can understand. Simply, as the issues regarding accepting the cookies on websites already well-proved, data controllers do not wish to provide such information. Also, data subjects' tendency to not well-reading the presented information makes it easy for the data controllers to avoid these obligations, since they only are interested in using the service rather than its details.[442] The GDPR itself does not entail the data controllers to provide information specific to AI systems which could be categorized as information about input data, the target values, and the consequences of the automated assessment[443]. There could be an argument placed here, on the difficulty to prove each data subject's understanding of the information, and how data subjects could be forced to read the statements, but as we will present in the Recommendation part, taking proactive steps could solve this issue from the core.

[440] Ibid., p.4.
[441] Sartor, 2020b, p.63.
[442] Boucher, 2019, p. 15.
[443] Sartor, 2020b, p.55.

2.2.5. Meaningful Information

The GDPR's interpretation on providing either ex-post or ex-ante information is subjected to another topic for a discussion, we examine the question of what information and according to whom that information should be meaningful, data subject-specific or in other words, person-specific information shall be provided, or the information should target everyone in the same way, as the practice is now. Simply, if the technology behind AI cannot be explained simply to the data subjects, they cannot exercise a free choice to give their consent. Let us imagine all the technical aspects of the social robots we referred throughout this work. Even if the data controller (developer or service provider, or any other actors) tries to explain the logic of the algorithm or the system functionality, would it ever be a complete explanation as the technology aşready itself is complex[444]? Even if the information is presented (because it must be presented), average data subjects may have no interest in any of that technical and complex information and may prefer the simplest and clearest explanation. Some data subjects who have technical knowledge may need more information and explanation, some may not wish to know any technical issues but just the risks specific to their own case. We could even give the terminological differences between legal and technical fields as an example. For example, the term transparency[445] does not mean the same thing for lawyers and for developers. Using the term transparency in the information package prepared for the data subjects with a technical background may complicate the understandability of the information[446].

Let us also imagine the average technology users around us. Some of them are not interested in any technology at all, while some of them are living only with technology. Those who live with technology also do not have to be interested in the technology itself, but only use benefit from the services offered via a particular technology. Nowadays, in a technology-immature society where people have tendencies to give up more personal data to use the newest gadgets more. They most often do not understand these new technologies[447], and the circumstances of any informed choice they might ever make changes rapidly[448]. They are not even aware of the possibility and the consequences of an AI device being always on-

[444] Karyda, et. al., p. 208.

[445] During the 15th International Conference on Intelligent Environments we participated in several presentations referring technical establishments of AI technologies. Several presentations used term transparency as a technical term, not a legal one. Later literature review showed that the situation is studied from this point of view, and the result is affirming our understanding. See, Felzmann, et. al., 2019.

[446] Kim and Hinds, 2006, p. 83.

[447] Misek, 2014, p. 76.

[448] Custers, et. al., 2013, p. 440.

listen mode[449]. The most recent Eurobarometer survey conducted in June 2019 about the awareness of the GDPR summarizes that 47% of the respondents do partially read and 40% never read the privacy statements because they either find them too long to read or find the statements unclear or difficult to understand[450]. While the numbers speak in this way, we shall once again think about the concept of the explanations and information to be provided referred in the GDPR.

Which personal data, from what source, and in what way it was considered by an algorithm is still a question for many researchers waiting for its answer; but what makes the situation even more difficult is the ML service providers' attitude towards not sharing the technical details (even if they could succeed at a certain level). For example, Carlini et. al.[451] tested an algorithm by querying the ML service containing the original training set (called as a type of membership inference attack) to find out whether a given data record was a part of the ML training dataset or not. Since data subjects have a right to be informed whether their data is processed in this way, Carlini's work could be an example of how the GDPR may not be clear in the application. The paper proves that if several parameters are in the right setting, ML service offered by the providers such as Google and Amazon as a black-box setting and used by anyone to create a model could leak information about the training dataset which may result in information leak about people in the training set. The authors drawthe attention to the fact that Google and Amazon do not inform the users of their platforms about such risks which we believe would then result in them not being able to assess the risks accurately. Article 35 of the GDPR, on the other hand, stipulates that data controllers (who in this case are the user of the Google's and Amazon's ML services) may not entirely assess the risks before they start using the platform. If data controllers are not informed about such risks and even more, if they are not allowed to check the learning algorithm and the architecture behind, they would unintentionally breach the GDPR rules.

However, our problem statement is not only related to technical constraints and data controller's manner but also related to lack of or insufficient regulations and difficulty to regulate diverse populations that AI systems serve[452] as a result of former reasons. Practically, the GDPR does not oblige data controllers to present understandable information and verify whether the data subjects understand the information at least at a certain level.

[449] Manikonda, Deotale, and Kambhampati, 2017.
[450] EC, 2019, p. 47.
[451] Carlini, et. al., 2018.
[452] Whittaker, et. al., 2018, p. 7 & p. 35.

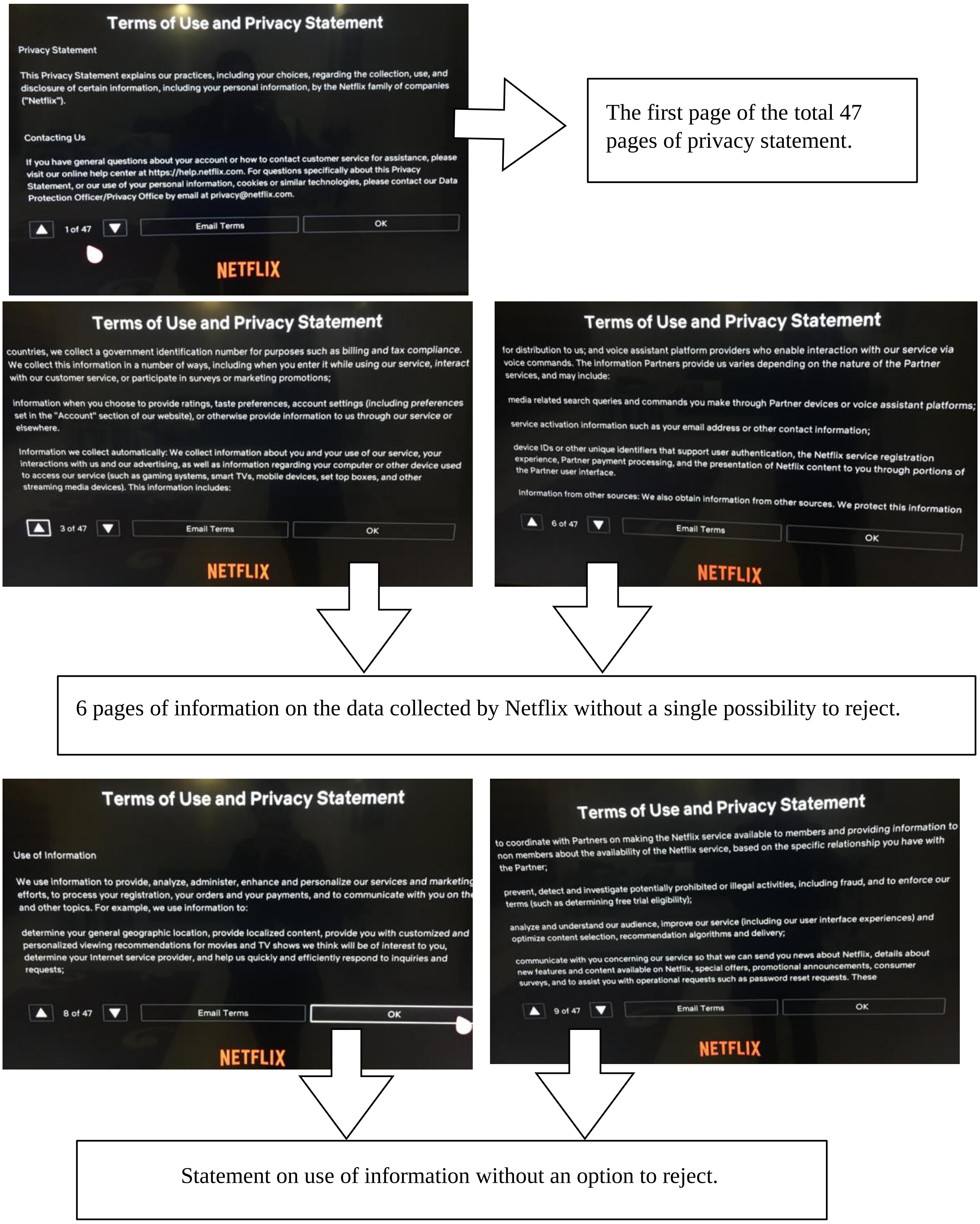
The GDPR, in fact, does not oblige data controllers to provide their data subjects the right to request explanation[453] in the right way. Unless there is no comprehensively thought and designed information and explanation on a person-based case, there will always be inconsistencies among the ways the information is delivered[454]. Data controllers are well aware of this loophole; one may recall what the Big Five (and their acquisitions)[455] have been practicing, changing their privacy and transparency tools in a way people would not understand or not be able to go for raising further questions. For example, YouTube still puts the "OK" button beside the "Review" button to trick the users, forcing them to accept its freshly updated (22 July 2019) privacy policy. Netflix (the largest online video streaming service in Europe) provides information about the processing of their users' data, but according to the privacy statement, Netflix uses any information related to the users leaving no possibility for them to freely decide to opt-in or even out. Non-exhaustive ways of collecting and using data without no choice to reject the collection of single data are not how the right to data protection in the EU should be in practice. Even though Netflix assures anonymization, in fact, only two non-anonymous reviews of a user made about a film in other related databases is enough to de-identify them[456].

[453] Wachter, Mittelstadt and Floridi, p. 95.

[454] Stats NZ, 2018, p. 34.

[455] "The Big Five Tech Companies & Their Big Five Acquisitions", Nicolas Lekkas, [Online], April 2019, GrowthRocks, Accessed from: https://growthrocks.com/blog/big-five-tech-companies-acquisitions/ Last accessed: 18 June 2019.

[456] Sartor, 2020b, p.37.



Terms of Use and Privacy Statement

Privacy Statement

This Privacy Statement explains our practices, including your choices, regarding the collection, use, and disclosure of certain information, including your personal information, by the Netflix family of companies ("Netflix").

Contacting Us

If you have general questions about your account or how to contact customer service for assistance, please visit our online help center at https://help.netflix.com. For questions specifically about this Privacy Statement, or our use of your personal information, cookies or similar technologies, please contact our Data Protection Officer/Privacy Office by email at privacy@netflix.com.

The first page of the total 47 pages of privacy statement.

Terms of Use and Privacy Statement

countries, we collect a government identification number for purposes such as billing and tax compliance. We collect this information in a number of ways, including when you enter it while using our service, interact with our customer service, or participate in surveys or marketing promotions;

information when you choose to provide ratings, taste preferences, account settings (including preferences set in the "Account" section of our website), or otherwise provide information to us through our service or elsewhere.

Information we collect automatically: We collect information about you and your use of our service, your interactions with us and our advertising, as well as information regarding your computer or other device used to access our service (such as gaming systems, smart TVs, mobile devices, set top boxes, and other streaming media devices). This information includes:

Terms of Use and Privacy Statement

for distribution to us; and voice assistant platform providers who enable interaction with our service via voice commands. The information Partners provide us varies depending on the nature of the Partner services, and may include:

media related search queries and commands you make through Partner devices or voice assistant platforms;

service activation information such as your email address or other contact information;

device IDs or other unique identifiers that support user authentication, the Netflix service registration experience, Partner payment processing, and the presentation of Netflix content to you through portions of the Partner user interface.

Information from other sources: We also obtain information from other sources. We protect this information

6 pages of information on the data collected by Netflix without a single possibility to reject.

Terms of Use and Privacy Statement

Use of Information

We use information to provide, analyze, administer, enhance and personalize our services and marketing efforts, to process your registration, your orders and your payments, and to communicate with you on th and other topics. For example, we use information to:

determine your general geographic location, provide localized content, provide you with customized and personalized viewing recommendations for movies and TV shows we think will be of interest to you, determine your Internet service provider, and help us quickly and efficiently respond to inquiries and requests;

Terms of Use and Privacy Statement

to coordinate with Partners on making the Netflix service available to members and providing information to non members about the availability of the Netflix service, based on the specific relationship you have with the Partner;

prevent, detect and investigate potentially prohibited or illegal activities, including fraud, and to enforce our terms (such as determining free trial eligibility);

analyze and understand our audience, improve our service (including our user interface experiences) and optimize content selection, recommendation algorithms and delivery;

communicate with you concerning our service so that we can send you news about Netflix, details about new features and content available on Netflix, special offers, promotional announcements, consumer surveys, and to assist you with operational requests such as password reset requests. These

Statement on use of information without an option to reject.

Figure 6. Terms of use and privacy statement by Netflix.
Source: Personal Netflix account.
Date of the pictures taken: 23 October 2019

In such an environment, the data controller of a social robot may tend to circumvent its stress to fulfill legal obligations by providing explanations that are not accurate or tricking its users like in the YouTube and Netflix examples or just prepare standard statements without assessing the person-specific conditions. Unless data subjects read the terms and conditions for products or services they use and unless all of them would read and understand the privacy statements fully, no valid consent could be obtained since they are not fully informed[457].

There could be even more reasons for such behaviors of the data controllers. They may prefer not to reveal their privacy losses to the users transparently, even if they implement privacy techniques such as differential privacy techniques, which also has its technical shortcomings in the implementation[458]. They may be having a fear of losing user's trust or they may not be wishing to show the shortcomings of their systems. On the other hand, since algorithms are developed with ML techniques performing tasks to find out the patterns in the data set which cannot be easily done and realized by human, or such realization may take months and becomes cost-full, the data controller may make up some stories[459] to make data subject believe in the information they provide. The problem here is that the data subjects cannot verify or nullify the accuracy of these explanations. Also from this point of view, the GDPR does not provide clear rules ensuring the data subjects' understanding of the legal basis in which the data processing activity is identified by data controllers. Data controllers' explanations are minimal, restrictive, not explicitly understandable by the data subjects (the logic involved with the algorithm), and finally, do not leave any chance for the data subjects to correct their behavior to receive the demanded decision in the future[460]. We could remember here once again the Netflix example given above. Netflix collects data from any possible devices in the broadest sense to use again in the broadest sense, and the users have no option to exclude some of the sources the company collects its data from.

In this case, would an informed choice through a single privacy statement giving general information about a social robot's system functionality which will not be read or understood be practically valid?

[457] Whitley and Pujadas, 2018, p. 30-35.
[458] Tang, et. al., 2017, n.p.
[459] Monroe, 2018, p. 12.
[460] Wachter, Mittelstadt, Russell, 2018, p. 878.

2.2.6. Intelligible Form

Previously, we presented a discussion on the fact that either technically, practically or legally, it is not easy to implement the informing obligation rules for data processing activities in AI systems. One may claim that the EU lawmaker already took many steps to ensure understandability of the information in the GDPR with the intelligible form requirement. Information in an intelligible form ensures data controllers to better fulfill transparency and consent principles. Although the word intelligible refers to the understandability (of the form of the information, in this case), years of practice with data protection legislation in Europe presents different perceptions on the concept. This probably is because no explanation had been placed in the GDPR regarding the meaning of the intelligible form before[461]. For this reason, the CJEU received several questions regarding the form of the explanation that would reinforce fulfilling the transparency requirement at the time when Directive 95/46 was in force. Explanation from the CJEU regarding Articles 7 and 12 of the GDPR further put obligations on data controllers to provide information to the data subjects about processing in an intelligible form, which is “a form which allows [them] to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that [they] may, where relevant, exercise [their] rights”[462]. This statement is particularly related to data subjects' right to obtain information on what data is being processed about them, and then right to request an update in case it is inaccurate. This is also applicable to the information obligation of the data controllers referred in Article 22.

In another case, CJEU refers to specific rights in which data subjects should be able to exercise in line with the right to access data concerning them. The Court stated that the “data subject has a right to have the data communicated to him in an intelligible form, so that he is able, to exercise his rights to rectification, erasure and blocking the data”[463]. In the GDPR, Articles 13 and 14 seem complementary to these statements and may give a clue on what an intelligible form is since types of information to be delivered by data controllers to data subjects are listed. When we take a look at all of those cases referred, and the Court’s

[461] Article 12 of the GDPR obliges data controllers to provide information to the data subjects related to their data processing activities in an intelligible form, but does not further explain what such form should mean for the data controllers.

[462] Joined Cases C141/12 and C372/12 YS (C141/12) v Minister voor Immigratie, Integratie en Asiel, Minister voor Immigratie, Integratie en Asiel (C372/12) [2014] Judgement of the Court, ECLI:EU:C:2014:2081, para. 57.

[463] Case C486/12, X [2013], Judgement of the Court ECLI:EU:C:2013:836, para. 28.

answers, we could easily realize that none of the listed information oblige data controllers to ensure the understandability of the information they present.

The updated guidelines of Article 29 Working Party on transparency[464] actually give some clues about preparing intelligible information tailored to different audiences, so that the information could be understandable by each group even though as an average. Although it is a guidance, not a legally binding rule, it still is an important document that could present a framework for how consent/transparency/informing obligation to be fulfilled. According to the guidelines:

> "The requirement that information is "intelligible" means that it should be understood by an average member of the intended audience. This means that the controller needs to first identify the intended audience and ascertain the average member's level of understanding."[465]

Such a statement should be thought entirely well for making it applicable in practice. The requirement for the provided information to be intelligible should mean that it should be understood by an average member of the intended audience in the GDPR. The guidelines also suggest that the level of intelligibility (not the level of users' understanding) could be tested with several methods that still may not ensure every single data subject's characteristic. An accountable data controller may already know the people they collect information about and it can use this knowledge to determine what that audience would likely understand ('calculated intelligibility'). For example, a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children[466]. On one hand, these assumptions are valid for accountable data controllers which might not always be the sure-case. It would be an illogical case to expect the automated decisions to be self-justifiable; always the human behind the decisions are accountable. On the other hand, the statement made in the guidelines may remain vague, if the service to be offered is a personalized one developed based on an algorithm learning from personal data. If the condition is to first evaluate the groups based on criteria such as age, there still could be quite big differences between the understanding level of people even within the same group.

[464] Article 29 WP_2016/679, p. 7.

[465] Ibid., p. 8.

[466] This even may not always be true. In the report prepared by the House of Commons Science and Technology Committee on the algorithmic decision-making, dr. Janet Bastiman says that even if the information was presented in a way involving the full structure, weighting, and training data making the algorithms, it might still not be understood by the end users. House of Commons, 2018, p. 28.

Recent experiences show that younger people understand specific terminology much better than older ones do, but not all the youngsters in the same way.

Focusing on the average data subjects might be quite challenging since the services an HSR offer is personal and is based on personal data. Recalling the philosophy of the informational self-determination and the importance of being able to decide as self, we find this simplification dangerous. Besides that, there are no criteria defined for data controllers to assess and identify the average groups, who belong to an average group, who not? What should happen with the persons who do not belong to the average group? (just like in the case of false positives and false negatives).

The EDPB suggests that a controller should take into account what kind of audiences they target the information with, but since the GDPR does not explicitly refer to the groups or types of data subjects (e.g., elders, persons with disabilities, youngsters, etc.) except children, their example cannot go beyond what the law says.[467] For this reason, we think that understandability of the information must be one of the main elements for proving the validity of consent obtained since it has an important role for data subject to make an autonomous decision about the future of her data because only if data subjects understand the risks[468], then they could make the risk assessment which the GDPR is based on. This assessment should not focus on a general data subject group, but also to specific groups who might be more vulnerable[469] when they use the robot and make decisions.

Besides all those arguments, stress should be made on the fact that some authors are referring back to the problems related to the difficulties of understanding the information, as we described above. Burrell[470] states that if the intelligible form would mean to ensure the data subject's understanding of the technology, it would not be possible to ensure this since it is not possible to understand the intelligibility of the algorithm. He further describes the reason for this statement, that the AI algorithms are far from programmability within the traditional meaning done with hand by a human.

[467] EDPB, 2020a, para.70.

[468] Schönberger, 2019, p. 190.

[469] One of the results of the ExplAIn project points out that 95% accurate decisions may prevail over the importance of right to explanation in case of health. This statement reveals the fact that right to explanation may be demanded based on a context, meaning that right to explanation may not necessarily be inserted in every system's field of functionality. ICO, 2019, p. 15.

[470] Burrell, 2016, p. 7.

2.2.7 Information for Vulnerable Groups

Thus far, we took a general approach to the data controllers' responsibility to obtain the consent of the data subjects', leaving aside the probability of the variety of the user types (that may potentially interact with a social robot). Recently, social robots are more likely to take place in children's and elders' life and take different roles in people suffering from different health problems, in the first place. Under the present title, we would analyze the GDPR's consent requirements specified for the potential social robot users, if there is.

Article 8 of the GDPR has dedicated to the child's consent in case the data subject is a child. While deciding the minimum age limit of a child is left to national jurisdictions, the scale for the age limit is chosen by the GDPR is from 13 to 16 years. Recital 38 gives a clear message about the reason why designating special conditions for a child's consent which "they may be less aware of the risks, consequences, and safeguards concerned and their rights concerning the processing of personal data". This is a very well-thought and justified reason by the EU lawmakers. In practice, if a child is the data subject, parental responsibility of the child should be ensured e.g. by verifying the age of data subject with a step by step approach. Some data controllers (as a service provider) designed strong tools for verification of data subject's age. They ask the parents' credit card number or ask for an e-mail address of the parent to send a verification email. Unless the parent consents for the child's use of that particular service, the service is not enabled for the child. Besides, many e-mail providers approved the age of the users of their services with such methods, so it is safe to say that the rule worked well in practice.

Related to consent requirements for a child, Article 12 of the GDPR stresses that information provided for a child should be "concise, intelligible and easily accessible form, using clear and plain language", in short, should be at such a level that a child could understand it easily[471]. As expected, a child should be fully able to execute her right to manage consent as it was referred to in Recital 65 of the GDPR. Supervisory authorities are specially designated duties related to the protection of children's rights under the GDPR, as Article 57 of the GDPR states.

Unlikely indicating the rights of children and specific requirements for a child's consent in the GDPR, there is neither specific consent requirement defined for persons with disabilities and elders not assigned obligations for data controllers in case data subject belongs one or

[471] Recital 58 of the GDPR.

both of these (vulnerable) groups whereas e.g. whether person is disabled and the whole related data concerning this status is categorized under health data[472]. There is reference neither in the GDPR nor in the Recitals regarding rights of elders or people with disabilities as data subjects. Especially for elders, one may not realize any special circumstance to regulate elders' data protection rights, but in case of social robots, and specifically for the ones designed for elder-care, could raise some concerns. This work does not aim to research data protection rights of persons with disabilities and elders, however, we must refer to this problem since these deficiencies surely become problematic when people belonging either of those groups start sharing their lives with a social robot which they need the robot the most, in the end, become dependent on them. Here again, the consent problem appears as the most significant problem.

We think that elders, people with certain health problems, and people with disabilities are more open to emotional manipulation by social robots which may encourage them to share more of their private life without assessing a different kind of the risks explicitly. Since regulations and rules designated for legal capacity of persons with disabilities may exceed the EU's competences (specific regulations on vulnerable rights are placed under national law or in other words, such regulations do not fall under the explicit competences of the EU), the GDPR's application on the protection of elders' and people with certain diseases data protection rights worth discussing deeper.

We could start illustrating the discussion with the following example; one could imagine a data controller generating privacy statements written in a standard way for anyone without differing data subjects based on their specific information needs whether they are a member of a vulnerable group or not. According to the current legislation, there is no obstacle for data controllers to fulfill their obligations related to informing activities in this way. On the other hand, elders (also people with certain diseases) communication with the robot may include many stories from the elder's whole life including very private moments. There might be scenes (e.g. bathing scenes), moments with families, or other private scenes that need special regulation and authorization from the elder person. Körtner[473] groups some of the ethical risks of robotics for elders as deception, dignity, isolation, privacy, security, and vulnerability. Regarding deception problems, he points the fact that differing robot's behaviors from humans might be even harder for elders than other people. The dignity of

[472] Recital 35 of the GDPR.
[473] Körtner, 2016, p. 305.

elders is more fragile since they might be more open to emotional manipulation. After all, elder people would only have the robot in their life and be only with them since they feel most comfortable when the robot is around. Unfortunately, the GDPR already did not solve the problem of the "one size fits all" approach for privacy statements and still does not provide specific regulations for elder's data protection rights. Moreover, we see all the problems raised for vulnerable' interaction with social robots as they could be also valid for anyone else. True of all, but all could be valid for any person at any age.

Until now, we ensured that the GDPR will be challenged with its exemptions already, but still applies to the data breaches regarding social robots at personal use. In addition to these issues, we illustrated how GDPR omitted regulation of certain rules for minors vulnerable who would be most probably the first receivers of social robots' services. However, we now step to the rules that apply to everyone promiscuously a particular group. We already mentioned difficulties to exercise the right to access information and consent rules, but we now step to the rules that are specifically engaged with social robots, as we may think.

2.3. Arguments on Algorithmic Black Boxes

One of the strongest arguments related to the obstacles before delivering explanations and sufficient information about AI systems followed by technical academia is the famous black-box arguments. We highlighted some of the discussions under the Meaningful Information, and Intelligible However, more insight could be helpful to have a better understanding of the topic both from the technical and legal points of view.

According to the arguments put by the technical academia, black-box algorithms may prevent even data controllers to first understand what algorithm exactly is doing with the personal data and how does it evaluate that data, so that data controllers may find themselves in a difficult situation when providing explanation or information. It is because they are bound to explain something to the data subjects that they do not even know how it works[474]. Let us imagine that all the legal and natural persons developing a social robot are required to explain all possible functions and capabilities of the robot. If the system used a type of supervised learning, there is a high possibility for data controllers to easily foresee the

[474] Director of the Institute for Next Generation Healthcare, Joel Dudley, made a comment on the algorithm that could predict successfully schizophrenia which is a difficult case for doctors, he found out that "We can build these models, but we don't know how they work." The Dark Secret at the Heart of AI, Will Knight, [Online], MIT Technology Review, 11 April 2017, Accessed from: https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/ Last accessed: 15 April 2019.

outputs of the system at a certain level. However, “this becomes difficult to implement as algorithms become more complex and unpredictable”[475].

Neural nets are not designed to reveal a “list or catalog of all learned information where we could have a look at the information that is stored inside the network, as well as see what information is not represented inside”[476]. Moreover, systems operating with RL techniques are operated in a highly dynamic environment where “errors are a necessity” for the systems to learn the right behavior.[477] The only way to see the error is to train the system first, then let it collect the data which will then be transformed into knowledge and only after all by testing and experimenting it. However, merging the training and learning phases, and due to its dynamic nature, the RL technique makes it impossible to always check and predict the outcomes of the system[478].

In fact, and according to the legal academia, the black-box problem does not only refer to the technical establishments but also the social fundamentals of AI. According to van Wysenberg, there are three types of black boxes in which the concept shapes so. The first one is, as the current work strongly highlights, related to the complexity of the technology making for average users difficult to understand how it works therefore cannot perform informed choices. The second black-box concept is related to the behavior of the institutions who may prefer not to disclose much information on how their system works based on whatever reason. Such institutions are, in the course of her works, refer to the intelligence agencies or the law enforcement bodies. In our opinion, the producer’s (company, engineers, manufacturer, etc.) tendency hiding information could also be inserted in this group. The final black-box is referring to the technical elements of AI that are unique to this technology, pointing to the automated decision making capability and ML techniques. These black-box concepts, without a doubt, conceptualize the problem of black-box more tangibly.

In our opinion, the technical issues could be overcome with the help of other technical opportunities. For example, Project exp*lA*in aims to define the obstacles before creating explainable AI systems and offers several solutions that could technically also be implemented. Another example could be that IBM recently announced an explainability

[475] Barfield, p.196.
[476] Matthias, p. 179.
[477] Ibid. p. 177.
[478] Ibid., p. 171.

toolkit[479], academia has been considering the topic closely[480], and have been producing several theoretical solutions[481], although these solutions mostly focusing on explaining the algorithms leaving aside testing whether human understands these interpretations or not[482]. DARPA[483] and Google[484], also effort to open the black boxes. We believe that soon there will be a solution for algorithmic black-box problems, but let us hope that the solution will not reflect another justification for data controllers to skip their legal obligations. The black-box related issues raised by the legal academia, on the other hand, could be solved with a more practical approach in which the Solutions part of this dissertation refers.

2.4. Is consent the only legal basis?

When we start examining the legal basis for social robots processing data, we realized that there are exemptions that might apply to the data controllers' some of the obligations. Although these exemptions apply generally to the legal persons, we think that social robots placed at-home serving to personal use would meet other individuals, besides the main user or users. In addition to conflicts regarding data protection issues between individuals and legal persons, individual to individual conflicts could also arise easily. In the following, we would like to show how and why a social robot at personal use cannot be exempted from the GDPR but how it could lead collision of two fundamental rights (right to privacy and right to data protection). Since we will examine some of the GDPR exemptions in our case, we found it useful to discuss the household exemption first.

2.4.1. The Household Exemption

The first and foremost discussion related to the GDPR's exemptions is not the household exemption, however, since this work focuses on the private use of social robots, it is worth discussing why and how the household exemption could be thought for advanced technologies targeting personal use. As the analysis will show, whether the exemption is

[479] "AI Explainability 360 Open Source Toolkit", [Online], IBM. Accessed from:http://aix360.mybluemix.net and https://xaitutorial2019.github.io. Last accessed: 12 January 2020

[480] "Special Issue on Explainable Artificial Intelligence", [Online], Elsevier. Accessed from: https://www.journals.elsevier.com/artificial-intelligence/call-for-papers/special-issue-on-explainable-artificial-intelligence . Last accessed: 12 January 2020.

[481] Ribera and Lapedriza, 2019, p.6.

[482] Tjoa and Guan, 2019, p. 13.

[483] "Explainable Artificial Intelligence (XAI)", [Online], Matt Turek, DARPA. Accessed from: https://www.darpa.mil/program/explainable-artificial-intelligence Last accessed: 15 January 2020.

[484] Some of the Google Brain team members run their researches in this field. See: Kim, et. al., 2018, n.p. (online). Accessible here: http://proceedings.mlr.press/v80/kim18d/kim18d.pdf Last accessed: 15 January 2020.

applicable, a natural person might be sharing some of the consent obligations of the main data controllers.

The main reason why the household exemption is placed both in the Directive 95/46/EC and the GDPR is the necessity to balance between the rights recognized in the data protection legislation. Thus, balancing the right to privacy against the right to data protection is a difficult task since the two rights are different but also interrelated, as was discussed in Part II. One of the methods that European lawmaker uses to balance these rights is exempting data processing activities which are aiming personal or household activities (hereafter: household exemption). The household exemption was originally presented in Directive 95/46/EC and was kept also in the GDPR. However, not many cases were yet brought to the CJEU giving a broader and clearer understanding of this exemption, but we expect more cases before the DPAs or national courts since personal products and services enhanced with AI in embodied form could easily take place at homes for personal use in near future.

Since there has been no court case brought before the CJEU after the 25th of May 2018 related to this topic, we could find paths to understand the household exemption only from the cases interpreted in the frame of Directive 95/46/EC. Though, the concept of household activity has not changed much within the GDPR. The second indent of Article 3(2) of Directive 95/46/EC and the third indent of Article 2(2) of the GDPR is the same word by word as following:

> "This Regulation does not apply to the processing of personal data…by a natural person in the course of a purely personal or household activity".

The GDPR's Recital 18 clearly states that the exemption does not apply to the natural persons who are subjected to purely personal or household activities, however, it applies to controllers and processors if they provide the means and purposes for processing data under personal or household activities. Compared to the Directive 95/46/EC, the GDPR's Recital 18 introduces terms such as "exclusivity of the processing," or "gainful interest" for deciding whether processing activity is household or not. However, the terms are comprehensive and not clearly defined in the legal text which might be confusing during the implementation.

The first draft of Recital 18 was designed in a way that the exemption would apply to all controllers and processors. The Council modified the draft as the exemption would not apply to the controllers and processors[485], and the possible reason for that it would cause a total

[485] Comparison of the Parliament and Council text on the General Data Protection Regulation.

dysfunctioning of the GDPR on today's personal based technology use. Our opinion is based on the Council's next step, which then added social networking and online activities into the quasi-list of household and personal activities. As a result, pure household activity in which purposes defined by a member of a family could not be evaluated under the household exemption, according to the GDPR.

The Recitals in regulations are not legally binding texts even though they were referred to in some of the Court cases which we discuss below[486]. However, they are important tools providing an understanding of the concept of the rules which then help the application. In this case, the final text of Recital 18 of the GDPR should worth to be placed here, as following:

> "This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities".

Since the GDPR focuses on the protection of individuals' data protection rights against legal persons, protecting individuals from the other individuals' possible privacy interferences may be less thought, even though the natural persons also could turn to be controllers. In this case, the responsibilities and liabilities of natural persons as taking either small or big part in data processing activities of certain technologies may fade away within the text. Especially, exempting the GDPR from individuals' household and personal activities without a clear definition and interpretation of the terms raise some questions in today's technology-dependent world. It is not crystal clear how the GDPR may help for an individual whose privacy was breached because of a robot placed at home and operating under a personal usage, and for an individual who operates a robot for such personal purposes such as healthcare. In case of breach of rights, finding out whether the user or the producer of the robot shall be liable in the capacity of data controller worth further analysis. During the years

[Online], Accessed from: https://edri.org/files/EP_Council_Comparison.pdf Last accessed: 17 January 2019

[486] In Planet49 case which was closed in 1 October 2019, AG Szpunar states that a "good legislative practice by the political institutions of the EU tends to aim at a situation in which the recitals provide a useful background to the provisions of a legal text". para71 of the Opinion of Advocate General Szpunar.
This means that if a Recital is considered in a case interpretation by the CJEU (in practice, in other words), it can have a legal meaning in a narrow sense.

of enforcement, the household exemption was practiced in the frame of Directive 95/46/EC in few cases. Some of the CJEU cases are interpreted in the frame of the household exemption which forms the basis for understanding its concept. These cases proved that natural persons could be indeed data controllers from different points of view and could be held liable as a result. Further, we will present those relevant cases where the household exemption was directly questioned, and which made an impact in relevant EU case law by adding a new element.

2.4.1. Household exemption for Household Social Robots

The cases brought to the CJEU related to household exemption are mostly related to old or already widely used technologies. No case related to the use of smartphones, IoT devices, or a social robot has yet been brought before courts (neither before a national court nor the CJEU). However, the data protection community of the EU already is aware of the fact that such a case could be difficult to interpret especially if natural persons are likely to be assigned some responsibilities as a data controller. Some below-given examples from the interpretation of the GDPR may help to explain this statement.

EDPS's opinion on cloud computing states that since it is the provider who provides the means for processing, the household exemption may not be applicable even if the service is used for personal purposes (of course, if this usage brings some financial benefits)[487]. In such cases, EDPS defines individual users as data controllers. Article 29WP further states that natural persons' responsibilities related to security requirements should be lighter than the providers[488]. Furthermore, natural persons as data controllers should inform other people about the existence of data processing, the legal bases for data processing, and they should comply with data protection principles. They should allow the data subjects to exercise their rights such as the right to rectification and the Right to be Forgotten.

In another opinion, the EDPS refers to the nature of the business model of the IoT and concludes that the user's data are systematically transferred outside of the scope of personal activities, therefore device manufacturers, application developers, and other third parties qualify as data controllers. In case of personal usage of an IoT device, the household

[487] European Data Protection Supervisor Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe”' (16 November 2012)

[488] Article 29 WP, 2013, p. 5

exemption will, therefore, be of the limited application[489]. This assumption may not seem fair since the risks of data processing activity do not arise from data processing activity of robot manufacturer, developer, or a third party, but may well be because of personal usage.

Finally, the WP29 provides a guidance to the natural persons to find out whether data processing activities they proceed with are under the household exemption, or not. This practical approach could be useful to understand the basics of household activities before they start to use particular services like what a personal robot could offer. One of the questions seeks an answer to whether "the potential adverse impact on individuals, including intrusion into to data subjects' privacy" is the case with data processing activity, or not. While all the other questions, (e.g., regarding the number of people whose data is disseminated, scale and frequency of processing activity, and the relationship between the individuals whether they are in a personal or household relationship) are pointing possibility of defining data processing activities carried by a personal robot to be personal or household activities, potential adverse impact is the only one which may not fit into this concept. In parallel with it, WP29 warns individuals to be careful about the data sharing activities of other people on mobile applications they use [490] . This might be evidence of how responsibility could exchange between legal persons and natural persons depending on the use of certain technologies.

Before finalizing, we would like to refer a comprehensive work where the household exemption was analyzed in the frame of current technologies at personal use. Butler's analysis[491] shows that purpose-oriented personal or household activity was unfortunately not considered in Directive 95/46/EC, therefore using drones for a personal hobby, or wearables for personal development, or taking pictures at school party may all be interpreted outside of personal and household activity exemption, although they might be interpreted oppositely under the national law of the UK. As the GDPR carries the same characteristics with the Directive 95/46/EC, and still not referring to purpose-oriented use of technology, having a personal robot serving personal use at home and home affairs may not protect individuals from some sanctions. In this case, difficulties to interpret cases related to the use of personal robots at home in a frame of the GDPR are expected, but in this work, we assume that such a robot should not be exempted from the scope of the GDPR.

[489] Article 29 WP_ 8/2014, p. 13.
[490] Article 29 WP_5/2009, p. 7.
[491] Butler, 2015, p. 8.

2.5. A Note on the Security of Social Robots

In some jurisdictions, e.g. Germany, "word privacy is sometimes used as a synonym for data safety in the area of protection of personal rights"[492]. Since we are not intending to make research on the privacy effects of unintended attacks to a certain system or about the data breaches related purely to system security issues, we will keep this part as short as possible.

Indeed, hacking and different types of possible attacks to AI systems are one of the most frightening events that may happen and cause issues not just from the privacy point of view but also the economic, technical, and even reputation of the data controller points of view. Developments in the robotics field go along the other technological developments, for example, cloud computing, production of sensors and other hardware, developments in network quality, all constitute some components of robotics. They all have their own degree of security risk. When one is analyzing the security issues related to AI and robotics, would always face different risks that the components of this technology bring both separately (risk belong to one specific component) and together (risks when they are put together). There are works in the literature showing how household robots are open for outside attacks and how those attacks seriously could damage people's privacy, for example, by leaking identification information, letting attackers enter into the home's network, camera and microphone interception which enable an attacker to sneak in video and audio streaming.[493] The security of robotic systems is one of the hottest topics in the robotic field.

Data controllers already need to take several security safeguards to protect their systems from attacks under the GDPR. Article 25 of the GDPR refers to the essence of secured systems from a data protection point of view and Article 32 of the GDPR states that "data controller shall implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, efficiently and to integrate the necessary safeguards into the processing to meet the requirements of this Regulation and protect the rights of data subjects". Further, Article 32 refers to the security of data processing stating that "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller, and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk". It refers to

[492] Leroux, et. al., p. 48.

[493] Denning, et. al., 2009, p. 105.

the security measures that should be taken based on the risks which should be assessed by the nature and amount of the data. These obligations are not always an easy task to complete for the data controllers. Even the models used in ML are not counted as personal data, since they consist of personal data regardless of they were pseudonymized or anonymized, they are entitled to the GDPR rules and obligations. It is also hard to prove whether an attack on the security of these systems was initially done to reveal personal data or not[494]. The possible security risks of using personal robots at households come with risks of being vulnerable to these attacks and it could not be solved by enhancing security in any technical meaning[495]. Technical constraints to understand and prove the nature of the attack may put the data controller in a stressful position to comply with the GDPR which remains abstract regulation for ML and AI. But in this work, however, we do not question the effects of unintended attacks on privacy.

[494] Veale and Edwards, 2018, p. 5-6.

[495] Denning et. al., p. 107.

VI. Analysis of the Research Questions and Expert Opinions

This section will be presenting the analysis of the questions and the arguments raised thus far. First, the scenario will be presented, then the scenario and the questions in the Appendix will be analyzed based on the related GDPR articles, CJEU cases, and other implementing documents. Next, the expert opinions on the scenario and the questions in the Appendix will be analyzed.

1. Scenario

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, doing more sports, learning science, and developing the 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, equal only to that of an Apple® computer made in 2019. Most of the people in Europe can easily afford a personal service robot enhanced with several Machine Learning 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, '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

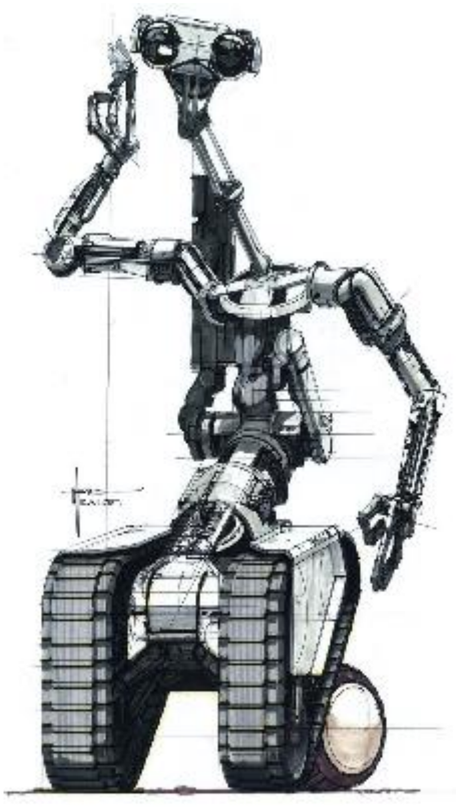


Figure 7. A futuristic robot.
"C Short Circuit Robot design by Syd Mead"
Downloaded with permission from:
http://sydmead.com/syd-mead-short-circuit-robot/

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[496] 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 Machine Learning research and technology investments made in this field a decade ago.

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 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[497], 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 to. 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[498]. She remembers

[496] Companies are understood as the entities producing, selling, and maintaining the robots, and dealing with few problems arising from personal use.

[497] This name consists of two words which one of them is robot and the other is "insan" meaning human in Turkish.

[498] 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 the House of Common Science and Technology

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.

While the installation was on-going, Julia felt exhausted with the 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 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

Committee's Report entitled "Genomics and genome editing in the NHS" generated in 2018. The report is accessible here: https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/349/349.pdf 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 what level of confidence 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.

After the HSR placed the second refill order for Julia's prescription medication, when she opened the delivery box, she 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 is the only one who interacts 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 the Robinsan used for prediction, they found some technical information that they could not understand much. He sent an e-mail to the Company asking an explanation, and the Company gave one saying that personal data might be collected in the course of placing food orders, or in preparing for the memory 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)[499]. The Company indicated that it was Julia who purchased

[499] During the first defense of this work, a critisizm was rased related to Robinsan's decision-making proceudre on Julia's son drug addiction, mainly, based on what data Robinsan could have came to the drug addiction outcome was not clear for the readers. So indeed, it was not clearly indicated in the scenario, except than the general rules such as the robot's accession and processing capability of physiological, psychological and emotional data that could be gained via face recognition or a small hardware that could portably measure

Robinsan and enabled it to collect data, therefore data collection means and purposes 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 some “unpredictable” results. The National Supervisory Authority is now preparing for an investigation, with several questions in the case file.

2. Preliminary analysis of the scenario

In our scenario, we assumed that Julia’s son first refers to the DPA (located in any MS) and then file a case before a local court. We believe, that such a case, as it would be the first of its kind, would be referred to the CJEU for a preliminary ruling. For this reason, before we analyze the expert opinions, we shall first present the analysis of the existed case law that applies to the questions we thus far referred to.

2.1. The Household Exemption Questions

We should first of all stress that we do not question Robinsan’s company’s data controllership issue, since it is quite obvious that the company’s data processing activities can never fall under the household exemption. We are confident about the fact that if such a case is brought before any court, the main company behind the robot probably would claim that it is not the only data controller, but the user also contributes to data processing, therefore, no full liability shall be applicable[500]. Therefore, we will below discuss Julia’s position whether she could be assigned any controllership since the case cannot be interpreted under the GDPR if it falls under the household exemption for Julia. There are two cases (Lindqvist and Ryneš cases) in which the household exemption was questioned

additional data. 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 (as seen, without an additional hardware). We could insert a 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.The experts interviewed were already introduced about these extras during the interview.

[500] In the Fashion ID case, Fashion ID claimed precisely that it could not be considered as data controller, but Facebook was the only data controller. C-40/17 - Fashion ID, para. 34. EP’s Resolution on Civil Law Rules on Robotics explicitly discussed the liability of to the user or the owner in case a robot causes a damage during its operation or is still learning. The statement continues with a note that in such a case, an assessment is needed whether the user is a professional user or not. To our view, it should be the producer or the provider who should train the user to gain the capability of using the robot professionally, but in this case, the user might have a degree of responsibility. EP, 2017, p.14.

from the natural person’s point of view, and there is a recent case that gave another dimension for a specific interpretation of the household exemption before the CJEU (Jehovah's witnesses case). Our analysis will show that the particular case we presented does not fall under the household exemption, Julia cannot be named as a data controller although there could be possibilities for her to be held liable in certain cases.

Bodil Lindqvist case

The household exemption rule was questioned for the first time in the Lindqvist case. It is not a coincidence, that the case was brought in 2002, the earlier years when people start using the internet for personal purposes. According to the facts of the case, Mrs. Lindqvist, a Swedish national living in Sweden, established a webpage for a group of her friends knowing each other from a parish. The website’s link was an offline link, meaning that it was accessible only by the ones who have it. Some, but a limited number of personal data of her friends, including their sensitive data such as data related to their health, besides their names and affiliation, was published on this website to keep acquaintance. Mrs. Linqvist once mentioned on the website that one of her colleagues injured her foot revealing the colleagues' health condition. Upon some of her colleagues’ negative feedback, she removed this information from the website, immediately. However, the public prosecutor brought a prosecution against her, based on the Swedish Data Protection Act, claiming that she did not notify the Swedish DPA about the website, she processed sensitive data without notification to the other users and transferred their data to third countries (the website provider probably was not located in Sweden). As she went through appeal procedures, the Swedish (Göta District Court) Court of Appeal referred several questions to the CJEU. One of those questions was regarding the household exemption, as follows:

> “Can the act of loading information of the type described work colleagues onto a private homepage which is nonetheless accessible to anyone who knows its address be regarded as outside the scope of [Directive 95/46] on the ground that it is covered by one of the exceptions in Article 3(2)?”

At the first stage, Mrs. Lindqvist defended herself in a way that what she was doing was related to her right to freedom of expression (freedom that cannot be restricted or regulated unless national law says), therefore the question could not have been evaluated under the Community law. AG Tizzano who submitted an opinion on the case in the same way as Mrs.

Lindqvist's to keep the case outside of the scope of the Directive 95/46/EC [501] was not followed by the CJEU. Since the case was evaluated only from the data processing by a natural person's point of view, Mrs. Lindqvist's claim was not supported by the Court. The EC took the position that the Community law should not be evaluated only as it was limited to economic activities connected to the four freedoms (freedom of persons, capital, services, and products) but free movement of data should also be considered as both economic and social activity. The EC stressed that the integration and functioning of the common market could be succeeded in by this way because free movement of data in the EU was guaranteed by safeguarding the protection of people's right to data protection in such particular cases too. The Directive 95/46/EC is not restricting the data processing activities, but giving a framework for legal data processing activities, such as stipulating data controllers to obtain data subjects' consent.

In connection with that, the EC stated that excluding Mrs. Linqvist's case from the data protection legislation would cause a large number of websites to (try to) be excluded from the application of the data protection law, which, in the end, would create several inconsistencies. The Court took a similar position with the EC, stating that excluding Mrs. Lindqvist's case from the Directive 95/46/EC would cause unsure and uncertain applications.

The Court then turned to the question related to the household exemption. The analysis of the Court compared the household exemption with the other exemptions, such as data processing activity in the course of a criminal offense, and interpreted the current case as the religious or charitable activities that Mrs. Lindqvist carried out could not be excluded from the such a scope. The Court anyway expressed 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."[502] Further, while she did not notify her friends about the existence of this website, she also missed the opportunity to ask their consent. Swedish DPA received no information about the existence of the website, either.

As a result, Mrs. Lindvist was punished on the basis that she did not obtain the consent of her friends and did not fulfill her informing obligations as a data controller.

[501] Opinion of AG Tizzano, Case C-101/01, para. 35.

[502]Ibid., para. 47.

- The case is particularly important from our point of view because it is the first case describing a natural person who was a user of a novel technology as a data controller. Our position is that, maybe, if Robinsan disclosed Julia's son's health condition to someone else, the household exemption would never be a question. In such, there is a risk for data to be not accessed, but to be obtained by others, meaning that household exemption should not be applicable for Julia.

To remember, the link of the website was accessible only by the ones who has it meaning that the website was operating offline. The EC's position on evaluating the offline link which "is accessible not only to anyone who knows its address but to anyone using a search engine"[503] is remarkable since it refers to the possibility of personal data on the Internet to be accessible by an indefinite number of people. However, this statement which indicates the web page to be accessible by anyone who knows its address raises a question, since Robinsan does not have any public link on the web, but as the company states, that anyone who consented for their data to be processed by Robinsan to get access to her data via a private link.

František Ryneš case

In the Ryneš case, the Court developed the interpretation of the household exemption by strengthening the idea that a natural person could be a data controller while they use certain technologies if it also records some part of public spaces. The case was brought before the CJEU according to the facts that Mr. Ryneš, a Czech national living in Czechia, placed a CCTV system monitoring the entrance of his home as well as some part of a public place around his home for purpose of his family's and his property's security because their home was attacked several times by unknown people. The system was working offline meaning that no data was transferred outside of Mr.Ryneš' home and he was the only person who had access to the system and data recorded. Right after another attack, he successfully identified the attackers via the system and initiated a criminal procedure against them. However, the Czech Data Protection Office claimed that Mr. Ryneš breached the Directive 95/46/EC since he did not fulfill his obligations as a data controller. These obligations were the consent requirements, the purpose statement, notification obligation, and obligation to report data processing to the Czech DPO, as all also referred in the Lindqvist case. Mr. Ryneš

[503] Ibid., para. 32.

counterclaimed that he placed the CCTV by his family's health and security, therefore the case should be interpreted in the frame of household exemption.

On the contrary, the Court was not in the same view as Mr. Ryneš. Firstly, the analysis of the Court stated that offline use of technology is not a criterion to apply the household exemption since it still identifies the people in an automatic meaning. This was the question referred in the Lindqvist case, too, so the answer was that either online or off-line, automatic processing of personal data is the keyword. Further, AG Jääskinen[504] pointed out that there was real damage occıring to the possible data subjects since recording other people's data outside of the home happened, even if the device was placed for strong personal reasons. Again, AG Jääskinen made a very important contribution to the interpretation of this case by indicating that placing a camera in which surveilling people (either inside or outside of the home) cannot be considered within the meaning of household exemption, but this does not mean that recording was illegal[505]. The recording activity was falling under the legitimate interest of Mr.Ryneš who established the camera only to protect his property, his and his family's health and life. Such a legitimate interest, however, cannot override the others' right to privacy and data protection, as the CJEU later stated in its decision.

Since the case was questioning only the household exemption, the Court did not take into account the claims regarding the obligations of Mr. Ryneš as a data controller, however, confirmed that he was the data controller. What should have Mr. Ryneš done, to fulfill his obligations as the data controller, was not considered to be referred to the CJEU.

- The Ryneš case carries several important elements for the interpretation of our scenario. First of all, Julia brings the robot home which can surveil not only her daily routines but also other people's entering home. Moreover, besides the Company, she is the one who can access data in Robinsan's system and make use out of it for her daily memory activities. Further, she is now in a position of knowing her son's drug addiction issue, and she may, based on her legitimate interest, could visit a doctor to seek a solution for her son. This may raise an issue for her to be counted as a data controller in a bigger possibility than what the Lindqvist case presented.

Jehovah's Witnesses case

[504] Opinion of AG Jääskinen, C-212/13 – Ryneš, para. 19.
[505] Ibid., para. 54.

Jehovah's Witnesses case brought another question to the discussion about the concept of the household exemption. The basic question referred to the CJEU was related to whether data processing activities carried by religious communities in course of religious activities would fall within the household exemption. As a result, the religious group, Jehovah's Witnesses Community, and its members were refrained from collecting personal data that occurred during the course of the door to door preaching activities of the people who are unknown to the Community. The Community collected data such as name, address, beliefs, and family circumstances of those people without their knowledge and to use them for further visits. Neither such preaching activities were requested by data subjects nor they were aware that their data was being recorded. Moreover, the collected data was shared between the Community's other members. The Court interpreted the case in a way that the data collection activity went beyond its purposes and referred to the risk of data share with the indefinite number of people as similar in the Lindqvist case.

This case is important for the strong emphasis on what AG Mengozzi makes it clear about, that just because the Community members enter into people's homes does not mean that the activity is a household activity, therefore household activity is not related to a physical location[506]. Thus, a critical approach to this statement claiming the activities occurring outside of the home but between family members may well fall within the scope of the exemption.

From the above-presented cases which significantly contribute to a clear understanding of the household exemption rule of data protection law of the EU, the following summary could be reached: Each case balancing the other fundamental rights with the right to data protection is not an easy task and especially if two very related rights, right to privacy and right to data protection are at the core of the case. In the case of natural persons' possible responsibilities deriving from data processing, this relationship becomes quite visible. In light of the case law, it is safe to say that the Court takes into account the risk of processed data by a natural person to reach an indefinite number of other people which would not be the case if the robot is only deployed at home for household use. The Court also considers that although the household activity is not related to physical settlements such as walls of the home of the data controller, if the data controller collects data from public spaces, then processing is surely not falling under personal or household purposes. To make a recording of the public space reasonable, the data controller must fulfill his obligations such as providing information,

[506] Opinion of AD Mengozzi, C-25/17 - Jehovan todistajat, para. 51.

obtaining consent, or creating grounds for withdrawing consent. This rule may be interpreted as people recorded by Robinsan considered to be falling in the public space since they are not belonging to the household, even if Julia's son is subjected to the evaluation. Either any DPA or a court interpreting the scenario would evaluate Robinsan's actual use space partially public and would consider the fact that people under Robinsan's surveillance must be informed about the operation of the robot at home. On the other hand, Julia, as the main user, would be under surveillance (just like the CCTV camera does) and even more, under the autonomous decision making of Robinsan. The Company of Robinsan shall inform both Julia and, maybe, the people entering the home subjected to the Robinsan's data processing, and should obtain their consent. How consent should be obtained and what information should be presented to the actual and potential data subjects to ensure the consent is valid will be the second part of our analysis. As well as these questions are important, how to obtain the consent of others will be then analyzed.

2.2. The Consent Question

Upon the claim that the Company failed to obtain Julia's and her son's consent, the Company now brings all the evidence before the Court, such as the privacy statement attached to the sales contract, signed consent forms, videos where consent was taken orally by the time of the updates were made, and the user manual provided to the users before their purchase. The company presents the off-line user interface they provide to the data subjects where could they check some more information about the data processing and manage it accordingly. From the company's point of view, it has fulfilled the informing obligation which includes presenting transparent information indicated in Articles 12, 13, and 22 of the GDPR.

The question of whether data controllers have to ensure each data subjects' understanding, which is not explicitly stressed in the GDPR, carries the discussion to another dimension. Based on this loophole, the Company followed the practices shown by the other data controllers who provide their services based on algorithmic calculations and not paying attention to whether the users would easily understand the information they provide. However, "the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, and their right to object to the processing of those data" [507], as AG Cruz Villalon once stated. In his interpretation, too,

[507] Opinion of AG Cruz Villalon, C-201/14- Bara and Others, para. 74.

ensuring the understandability of the information is a missing point, but pointing to the huge responsibility of data controllers in safeguarding the data subjects to exercise their rights. This concept was later developed after the GDPR entered into force as we will prove below.

From the Robinsan's Company's point of view, it may be claimed that it does not have any chance to explain the purpose of Robinsan in any way, else than stating that "Robinsan is your friend who learns from you and serves you to fight against Alzheimer's disease. We created Robinsan's basic algorithm, but what it can do for you depends on what you teach it". The Company could believe that a technical explanation would not be understood or even of interest in the data subjects. Moreover, it may refrain from stating that the algorithm may end up with unpredictable results, basically, not to fear the potential users. Besides, the Company could prove that each data subject was instructed on how Robinsan works, how it could repurpose their data, and could reach unpredictable results. The Company, all in all, thinks that it delivered all the necessary information listed under Article 13 of the GDPR (name of the controller, purposes, etc.) and made the users aware of the existence and unforeseeable consequences of ADM in line with Article 22. In this case, since the GDPR does not oblige data controllers to prove whether the data subject understood all these explanations or not, the applicant should not claim that the company failed to obtain her valid consent.

We think that, based on the data controllers providing online services, ranging from a simple website to social media tools, or from specific websites such as shopping or online film services, presenting a one size fits all statement and a consent box where data subjects opt-in via clicking on "I understood" box is an illusionary and tricky practice that must be prohibited. Two very current cases interpreted by the CJEU may support this view.

In the Planet49 case, two questions that are at the utmost importance for our analysis were referred to the CJEU; one of them was related to the concept of the data controllership and the other one was regarding data controllers' duty to fulfill informing obligation based on the Directive 2002/58/EC on privacy and electronic communications[508]. The case was

[508] The referring Court asked the following precise question to the CJEU which is pointing an important deficiency on the interpretation of the data protection legislation: What information does the service provider have to give within the scope of the provision of clear and comprehensive information to the user that has to be undertaken in accordance with Article 5(3) of Directive [2002/58]? Does this include the duration of the operation of the cookies and the question of whether third parties are given access to the cookies?' Although the question seems only seeking for an answer for whether the duration of the operation of the cookies and the existence of the third parties should be communicated to the users, interpretation of the information to be communicated to the data subjects still lacks a comprehensive concept. Besides, new technologies, like the cookies in the Planet49 case, brings new challenges on the interpretation of the concept of the informing obligation.

brought before the CJEU since the Planet49, an online gaming company, placed two pre-ticked consent boxes to conclude a consumer lottery agreement on its website which enables cookies to collect personal data from the website visitors' devices. The referring Court (Higher Regional Court, Frankfurt am Main, in Germany) firstly asked the CJEU about determining what information does the service provider has to give within the scope of the provision of clear and comprehensive information to the user. In the analysis of this case, AG Szpunar[509] pointed out an important aspect of cookies which carries a certain complexity refraining the average internet user from fully understanding how the cookies are functioning as it is already something very technical. Moreover, the AG stated in his opinion, that if the data controller does not present sufficient information to the data subjects, this puts data subjects in an asymmetrical situation[510] (before the provider) who already rarely checks the content of the pre-ticked boxes offered online[511]. However, the user must be able to assess the consequences of the data processing activity and then give consent, therefore should be fully informed before the consent was obtained. The AG's position was adopted by the Court who further emphasized that the consent text should be presented "with sufficient clarity from a typographical point of view"[512] to ensure that the data subject has realized the consent boxes. Besides, the Court pointed the rules regarding storage and duration of the data to be processed, as this information should also be provided to the data subjects, although these were not included under Article 10 of Directive 95/46/EC. These rules were later included and made clear in the GDPR[513].

Finally, the CJEU stressed clearly that the pre-ticked boxes refrain data subjects from reading and digesting the information, and this practice raises the risk for data controllers to verify that the information was read otherwise invalidating the consent to be unambiguous and freely given[514]. In our scenario, Robinson's company should make an exceptional effort to ensure whether they provide sufficient information to Julia on the functionality of the robot and its AI-brain.

[509] Opinion of AG Szpunar, C-673/17 - Planet49, para. 114.

[510] Prohibition for data controllers to make consent statements causing imbalances between the data subject and the controller is placed in the Recital 43 of the GDPR.

[511] Ibid., para 37.
Lynskey, 2011, p. 880.

[512] C-673/17 - Planet49, Judgement of the Court, para. 35.

[513] Article 13, point 2 incident a requires data controllers to present "the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period" tothe data subjects.

[514] C-673/17 - Planet49, Judgement of the Court, para. 62.

Besides the question related to the interpretation of data controllers' informing obligation, the referring court asked whether the data controller should obtain the consent of the data subjects to store and/or gain access to information already stored in users' devices via cookies. The Court gave a clear answer to the prohibition of data controllers to access such information without the users' consent.

- If we turn to the scenario, and as we mentioned at the end of the analysis of household exemption, it is crystal clear for data controllers to obtain the consent of Julia but also other people about processing their data automatically recorded by Robinsan once they entered into Julia's home. If Robinsan's company plans to use this data for, e.g., commercial purposes, the Company must obtain a separate consent. If Julia forces people entering her home to accept the robot around them, Julia must be the person who obtains a separate consent besides fulfilling her informing obligations. What information to be provided to the potential data subjects and what information the Company should provide to the data subjects remains vague, due to the complexity of assessment of the functioning of robots, and there is no case yet assessing the concept of the information to be provided to the data subjects in case ADM is deployed in an embodied machine. For example, there could be a question whether only the clear purposes, or also the possible purposes should be communicated with the data subjects, or unless the purpose is unborn, there should not be any communication in this sense. Is there any possibility for data controllers to provide sufficient and understandable information on the functionality of the ADM which changes based on the inputs data subjects put through everyday interaction? We will assess these and more questions during the analysis of the interview results.
- On the other hand, Julia's son is not the person who directly benefits from Robinsan's services, so why would he be under Robinsan's evaluation? Robinsan is, apparently, a lack of distinction between the main beneficiary of the system and the others who are not and who do not wish to be. Would such a situation be against the data protection by design rule? From our point of view, clearly yes. Such data collection must be avoided especially if there is an AI system that can easily collect and evaluate any data. However, if the other persons gave their consent even though they are not the main beneficiary of the services of Robinsan, but to support Julia's treatment, and still they receive the services, then it may be considered against the granularity

element since the service “involves multiple processing operations for more than one purpose”[515].In this case, how to avoid processing the data of other people or how to legitimize it remains as one of the hardest questions for the AI community. Besides anonymization and data minimization rules which still require a degree of data processing (meaning that the GDPR still is applicable), there is no other clear solution available; they would keep relying on the consent rule which does not help them to fully comply with it. Personalized service needs personalized consent, and in some cases, explicit consent is the solution for such cases. This points to the clear necessity for the main beneficiary to collaborate with the (main) data controller in assisting to reach the other possible data subjects.

2.3. The Liability Question

“A social network, like any other application or program, is a tool. Similar to a knife or a car, it can be used in a number of ways…But it might perhaps not be the best idea to punish anyone and everyone who has ever used a knife. One normally prosecutes the person(s) controlling the knife when it caused harm.”[516]

We proved that informing obligation must be fulfilled by data controllers to legalize data processing activities of Robinsan. The GDPR has slightly changed the concept of the data controller, by introducing a more detailed description and more obligations for other data controllers else than the main data controller. Technological developments make a clear identification of data controllers involving and sharing responsibility for data processing activities complicated, and AI technologies complicate it even more. Ever since social media entered into people’s lives, many questions on the clear identification of liable persons using such tools have been a question under law. One of those legal questions belongs to the data protection field, according to the CJEU cases. For example, whether an administrator of a fan page established on Facebook would be a data controller was once referred to the CJEU as a preliminary question in the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (shortly, Wirtschaftsakademie). The Court held the position that there is no doubt on Facebook’s position as a data controller since it decides about the processing purposes and process data via cookies. But it is the fan page’s administrator who gives Facebook a chance to reach those purposes by triggering the

[515] EDPB, 2020a, para.42.
[516] Opinion of AG Bobek, C-40/17 - Fashion ID, para. 90.

data controllers to visit the fan page. On the other hand, the fan page administrators indeed gain benefits from this activity, such as learning about the audiences, so delivering better advertisements for them, and use also for statistical purposes besides assisting Facebook to reach its purposes. In fact, “processing could not occur without the prior decision of the fan page administrator to create and operate a fan page on the Facebook social network”[517] and we adapted this sentence to the present situation as: processing could not occur without the prior decision of Julia to purchase and operate Robinsan.

In the Robinsan case, it is very clear that processing would not occur if Julia never had Robinsan at home. Her benefit from the Robinsan purely triggers improving her health conditions. The company also strongly claims that they are not processing data outside of this purpose, and all data processing activities that might ensure this purpose are not under their control since Robinsan makes the decisions itself.

In the Robinsan case, the Company uses the data for assisting algorithms to make personalized services for Julia, and Julia triggers this activity in return for making a benefit of it (personalized health care). Although Julia does not process data herself, he uses automated tools to process data. Would it make her a joint controller or it would assign a degree of responsibility to her as a data controller?

The CJEU in the Fashion ID case made a precedent interpretation on the role of joint data controllers on their obligations specific to informing activities and obtaining consent. Facts of the case summarize, that the online retail shop Fashion ID once embedded a Facebook plug-in to collect “Likes” from the people who visit the official website. Such a plug-in, either the website visitor hits the Like button or not, and independently from the visitor’s Facebook use, helped Facebook and its parties to collect personal data of the visitor via the browser. The German public service association, Verbraucherzentrale NRW, filed a suit against Fashion ID claiming that placing this plug into their website gives the company a responsibility to obtain the visitors’ consent. Further, the company should also have informed them about the existence of such data processing to obtain valid consent. Fashion ID, as the data controller, argued that it could be named as a data controller since it had no means of controlling the personal data of the website visitors. In the preliminary request referred to the CJEU, Fashion ID’s position as a data controller has been questioned, besides

[517] C-210/16 - Wirtschaftsakademie Schleswig-Holstein, Judgement, para. 56.

other questions. AG Bobek started his analysis with an effort to identify the data controller(s) in the case.

AG Bobek first drew the attention to the fact that divergent opinions were raised regarding who was the data controller and to whom should have the consent was given to[518]. According to the applicant, it is the Fashion ID who embedded a Facebook plug-in on their website, so it should have obtained the consent of the data subject because non-Facebook users' consent was not obtained before. However, Fashion ID claimed that the consent should have been obtained by Facebook (headquarters located in Ireland). Following the Irish DPA's interpretation who indicated that the case was not about who should have obtained the consent, but how it was obtained (whether free, specific, and informed). The Polish representative was in a view that the consent should have been obtained either by Fashion ID or Facebook Ireland since they were both responsible for the processing. The Italian representative stated that the consent must have been given to both of them. Belgian DPA and the EC stated that it was not clear per the Directive 95/46/EC who should have obtained the consent. The Court took the position that Fashion ID facilitates the data collection even though it does not have any control over the data after the transmission[519]. These arguments would anyway be the same if the case was interpreted under the GDPR, besides, a new rule on data processors to obtain consent was introduced.

Apparent under this case, informing obligation was related also to the existence of the plug-in, and the data controllers should have provided information about it besides the other general information related to the plug-in. Fashion ID, however, did not provide any information to the data subjects neither before not after the data collection via that plug-in. giving as a reason that Facebook was the only data controller. However, the consent should first have been obtained by Fashion ID since the visitors first consult with its website which triggers data processing[520]. In this case, we believe that Julia should at least inform people about the existence of the robot, what data it may 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. For this to become logical, Julia first should be aware of this obligation, but can a simple user always be in such a situation?

- As soon as people visit Julia interacts with a robot (by entering into a conversation or only by being around the robot which records their videos or photos) they become

[518] C-40/17 - Fashion ID, Judgement, para. 88.

[519] Ibid., para. 74-75.

[520] Ibid., para. 102.

> data subjects whose data is being collected via the possibility that Julia brought by placing the robot at her home[521]. Julia is the beneficiary of the robot and is a decision-maker, even in a limited capacity, about the purposes of use. Due to the robot's capability to record personal data through profiling them and assessing their certain and unknown aspects to be disclosed to the others, the responsibility of the data controller (either Julia or the Company) is greater.

Should everyone who uses social media should be responsible for their actions, therefore the protection would be more effective, as the AG Bobek asks[522]. How to identify the joint controller, for this reason, is the most important step since the interpretation of the rest of the case would depend on identifying them clearly and then their responsibilities. AG Bobek in his analysis referred back to the Wirtschaftsakademie and Jehovah's Witnesses cases which concluded the joint controller concept in a general meaning referring to who made a collection of personal data possible[523]. However, the AG did not find this criterion specific enough giving a reason that it could pave the way any user of social media or other technological tools to be potentially held liable[524]. The AG summarized his opinion on the possible liability of any user, including the other parties in the personal data chain which do not directly trigger data processing directly such as internet service providers, to be very restricted, or even to be avoided. Still, the AG accepts that the GDPR broadened the definition of a controller which could result in some natural persons to be co-responsible for data processing. While the AG's opinion was not regarding a specific question referred to the CJEU, we are unsure whether the CJEU would consider it in the future in case a specific legal analysis is needed.

The Lindqvist case could be recalled here since it is the first case where a natural person was found liable under the Directive 95/46/EC. However, the problem with the Lindqvist case (and so with the other similar cases) was that what obligations a natural person as a data controller has never been questioned. Neither in the GDPR nor any guidelines, no specific explanation on what should natural persons do as data controllers for fulfilling their duties

[521] Ibid., para. 78. Fashion ID is the liable party triggering the data processing for Facebook by placing the plug-in on its website. Julia, may also be, "exerting a decisive influence over the collection and transmission of the personal data of visitors" to her home to the provider of Robinsan, which would not have occurred without operating Robinsan at home. Moreover, the paragraph continues referring to the liability of data controllers including natural persons' role on determining either the purposes or means of data processing assisting to the overall of chain of processing. We are aware of such interpretation would indeed be an extensive one, but still might be challenging the national courts.

[522] Opinion of AG Bobek, para. 71.

[523] Ibid., para 36.

[524] Ibid., para 73.

were mentioned, although the cases were concluding a certain liability of the natural persons. Indeed, their duties are not clear since their obligations are unknown. Do they have the same duties as companies like Facebook? How could Robinsan’s Company and Julia share the liability or should they only share some responsibilities? The idea of establishing an agreement between them seems even more chaotic since, by the time of conducting this research, we did not find any case where a natural and legal person agreed to be a joint data controller and sign an agreement with clear responsibility division. This means, that there is a lack of practice in this sense. On the contrary, Article 26(3) of the GDPR gives data subjects to exercise her rights ‘in respect of and against each of the controllers’ without such a practice. In the Robinsan case, it would be illogical to expect Julia to guarantee her son’s rights granted in the GDPR. Such an unclear issue is unfortunately opposed to the philosophy of data protection law which should protect people’s rights proactively, not enter the picture after the breach happened since once data is processed, it is impossible to undo.

3. Expert Opinions

In this section, we present the results of the interviews conducted with the experts in the frame of the scenario and the questions deriving from the theoretical part of this work.

As described in detail in the methodology section, expert opinions were collected via face to face interviews by visiting the experts. The visits took place from 10 November 2019 until 6 December 2019. In total, 15 experts delivered their opinions on the pre-established questions. Analysis of their answers will be presented firstly as a general evaluation, then it will follow the analysis of specific questions. Differences and similarities will be highlighted at country-based, and no expert name will be disclosed during the analysis. If it is necessary to directly quote from the interviewee, the quotation will be presented in the “Expert A, from (country X)” form.

To keep unity and ensure better understandability of the analysis, as well as to ensure the anonymity of some of the experts upon their request, we use the following coding presented in Table 2. during analysis. The codes are randomly representing the experts, and the letters assigned before the numbers shall represent the country the expert is from.

It will be indicated during the analysis whether the expert opinion is from the practical or from the supervisory authority point of view.

Finland	Hungary	Italy	The Netherlands
Expert F1 Expert F2	Expert H1 Expert H2 Expert H3 Expert H4 Expert H5 Expert H6	Expert I1 Expert I2	Expert N1 Expert N2 Expert N3 Expert N4 Expert N5

Table 2. Codes assigned for the experts to be used in the analysis

In general, we did not observe significant differences among the experts' opinions specific to their affiliations, but some of the questions were answered significantly different by the experts from specific countries. This will also be indicated, when necessary.

3.1. General Evaluation

Under this title, we focus on the expert feedbacks regarding the general evaluation on the scenario, specifically, what do they like and what do they dislike about the scenario; whether such a technology referred in the scenario would become real or available within 20 years; their opinion on the applicability of the GDPR on AI technologies in general; and other issues outside of the questions, but still related to the present work.

Most of the experts (12 experts in total) found the scenario an intelligent and gradually evolving scenario making the reader keep thinking about the borders of the application of the GDPR on new technologies. Most of the experts also indicated that the scenario looks futuristic, but it has many realistic elements that are happening even now. They like the scenario because it shows well the usefulness of the technologies, but also unexpected negative effects they bring. Expert N1 said that the scenario mentioned the right aspects of the existed problems and future risks of robots when (will be) used by people. Expert N3 and H5 said that the legislator could see whether the legislation is effective or not with the help of this and many more like this scenario before it is too late to act. Expert N5 said that it was more worrying to see how human intervention faded away during Julia's and her son's interaction with Robinsan.

Expert F2 noted that the scenario refers to the relevant aspects of the GDPR very clearly, for example, the problem with the sustainability of the consent, people's tendencies on refusing the possible risks of certain technologies, and problems deriving from data processing in ubiquitous environments. Expert F2 also referred that technology's ability to serve the wellbeing of people is remarkable and is well highlighted in the scenario. This view was shared also by the Expert H4. Furthermore, some of the experts indicated that the scenario brings the legal, practical, social, and technological perspectives together (shared views by the Experts N3, N4, H2, H3, H4, F2). Specifcially, and to conclude their opinion, Julia's dependent on a social robot makes an impact on her life greatly and makes her forget about the company behind Robinsan plays the social aspect of this technology making the story also a legal one. This was one of the targeted aim with the issues pointed in the scenario.

Expert F1 noted that this is the expert's favorite scenario, but prefers to remain optimistic from the point of view that humans had always dealt with the technology well at some level. The scenario reflects what is going to happen in the future, but there are always be human rights, privacy, and institutions protecting these values. The scenario indeed looks worrying, but the Expert F1 thinks that questions referred to in the scenario would be handled correctly.

The elements that the experts did not like in the scenario are quite a few, and are listed below:

- Expert N1 and N4 indicated that Julia's son's drug addiction and its discovery by Robinsan were unexpected for the expert. The expert noted that it took some time and some reading to understand the connection. Expert N1 also noted that the situation will be even more complicated in real life, so it might have been better to involve the other persons engaging data processing in the scenario. Our position is that we would not have intended to make the scenario more complicated which would then make it impossible to interpret for the experts. We also aimed to know what persons the expert would identify already, as referred to in Question 6. We consulted the experts orally about the data processing and decision making rules of Robinsan during the interview.
- Expert N3 noted that the scenario could refer to some broader principles such as Article 8 of the ECHR and the Charter of Fundamental Rights of the EU.
- Expert N5 indicated that it was hard to see the real problem in the scenario. The Expert N4 could not identify the problem clearly whether it was the drug addiction or Julia's experience with the company. We explained the expert, that both of them are jointly referring to the different problems subjected to the analysis in the scenario. Our explanation was welcomed by the expert so the analysis went on further.

- Expert H1 did not agree with the scenario that it would happen exactly as it is. Specifically, the expert does not believe that people would easily buy those robots in the future if they do not trust them. Still, the expert believes that the average user still would be acting as illustrated in the scenario.

Besides the specific feedbacks, we received some general feedback on the scenario from some of the experts. Expert F2 did not evaluate the scenario, but the problems referred to in the scenario that are real and need to be solved immediately. Expert F2 evaluated the consent, replacement of humans from social concept, and lack of transparency of data processing as the negative elements in the scenario.

Expert I2 also evaluated the scenario in essence, instead of making a general evaluation. Expert I2 indicated that these technologies are very important for human life, and sometimes it is the privacy that we pay the price for, as it was clear in the scenario.

Expert N4 gave the same general interpretation on the elements of the scenario which are the fact related to the user becoming more dependent on a single vendor (referring to the use of a single central database in the scenario) for receiving a health-care. Expert N4 referred to the current practices of the tech-giants making the users addicted to their services and changing their privacy policies in which leaving users no option to refuse, but just to accept.

3.1.1 Opinions on the timing of the HSR

Most of the experts (10 experts in total) delivered their opinions in a way that such technology referred to in the scenario either already has already been happening or would happen within 20 years. Expert I1 said that the next industrial revolution would occur within 10 years and the changes would even be faster than the past. Expert N1 noted that such robots (with limited capacity) have already been introduced in the Dutch hospitals for children care[525]. Expert N1 also noted that these robots make life easier, so people soon will adopt them easily. The expert also indicated that many consent pop-ups make the user

[525] There is no specific implementation, but we found several project based introduction of the robots at the Dutch hospitals. A robot interacting children with diabetes and a project under the TU Delft aiming to introduce robot-friends at hospitals could be given as an example.
"Robots interact with children to help with their diabetes", [Online], Euronews, 13 March 2017. Accessed from: https://www.euronews.com/2017/03/13/robots-interact-with-children-to-help-with-their-diabetes Last accessed: 28 January 2020.
"A robot friend for ill children", [Online], TU Delft, December 2016. Accessed from: https://www.tudelft.nl/en/eemcs/current/nodes/people/a-robot-friend-for-ill-children/ Last accessed: 14 December 2019
There are many scientific researches on introducing robots at children hospitals in the Netherlands. The latest one belongs to Moerman, Heide, and Heerink, 2019.

difficult to use the services of Robinsan properly. Expert H5 thinks that the technologies referred in the scenario exist separately, but will be once put together in at least a software form within 10 years.

Expert F2 noted that Robinsan may be real in 20 years, but not in 10 years for sure. Two of the experts (one from the Netherlands and the other from Italy) indicated that they could not foresee whether it would be real, but they were aware of many ongoing promising pieces of research towards.

3.1.2. General evaluation of the Application of the GDPR on AI technologies

The GDPR is fully applicable to the scenario we presented, according to all experts interviewed. Besides, all experts, without any doubt, stated that there is no need for amending the GDPR for answering to the questions related to AI technologies, and the other legislation such as the long-awaiting e-Privacy Regulation, consumer protection law, competition law, civil law, and criminal law could sufficiently cover AI technologies. No more law is needed since it complicates the implementation more (indicate by the Experts N1, I1, F1, H2, H3). The experts agreed on the fact that implementation of the GDPR and the future case law would clarify the application on AI technologies, too. Expert N1 raised the example of block-chain technologies which took so long to interpret the GDPR on. Interestingly, Expert N1 and N3 delivered an opposite opinion about the suggestion on generating more guidelines for the implementation, while the former referred that they were an important part of the implementation, and the latter stated that the guidelines were useless since they are not legally binding documents. It was also remarkable when the Expert N1 did not refer to the Dutch DPAs guidelines, but the EDPS guidelines explicitly.

In this case, problems regarding the application of the GDPR and the general issues on AI technologies were referred comprehensively by the experts. Expert I2 referred that the technology develops so fast, and lack of a common definition on the terms that the technology brings every day may make the right implementation of the legislation on those particular technologies (such as cloud computing, Big Data) quite hard. Also, the definition of the user, whether she was a data subject, patient, or a customer could complicate to find the suitable legislation to take into consideration in the application. Which rule is to apply to the particular case will be a future problem, especially since the GDPR is not going to be implemented by the national judges in the same way, as the expert stated. Some of the experts indicated that this could be tackled with the general principles referred in the GDPR, such as the principle of fairness, accountability, transparency, and they sufficiently can apply to the new technologies like AI (Expert I2, N5, F1, H4, H5). Expert F2, on the other hand, stated that AI is difficult to regulate with the general rules hindering the EU's innovative power in this field. The expert believes that it would take almost 10 years for the GDPR to be harmonized, based on the different interpretations of the national judges[526]. Expert H5 identifies the GDPR as a barrier for the profit companies until the NSAs gains expertise on certain technologies such as AI technologies, and the motivation to go after those companies breaching the rules without being exhausted.

Expert N3 identified the lack of clarity in the wordings of Article 22 of the GDPR when ADM "produces legal effects concerning him or her or similarly significantly affects him or her". For the expert, it is not clear how the significance of the legal effect could be defined by the courts and this would be the first challenge for the courts to deal with.

Expert F1 and N4 noted that besides the GDPR, a lex specialis could also apply to the questions referred to in the scenario. The Expert F1 pointed out the fact that Robinsan was a medical device and there were related Directives[527] applicable on devices in such (although they have not yet been updated in line with the GDPR). Expert N4 thinks that there could be a law regulating the AI technologies and the GDPR could be amended in line with that.

Expert N3, N5, and Expert H1 said that, since the AI does not always deal with the personal data, it excludes the GDPR from the application. Especially, training data may not fall under the GDPR in the beginning, but there could be many personal data/ outcomes based on training data. In this case, it is a question of whether the GDPR would only be applied to the output or also on the input, as we discussed and concluded that the outputs also should be considered as personal data.

Expert H1 stated that there is a need for drafting a new responsibility scheme for clear identification of the data controllers (not only related to AI technologies but in general). Data

[526] Expert F2 gave the example of Estonian approach which lets data protection legislation to be applied more casual based on the Estonian government's technology oriented political agenda. In the Nordic countries, as the expert stated, that the way GDPR's implementation will have more business focus, such as the case in the US. The expert further stated that the US has even stricter privacy rules than Europe in certain cases, for example, children's consent.

[527] These directives are quite old-dated; since 1990 technology in medical sciences has also been drastically change.
Council Directive 93/42/EEC of 14 June 1993 concerning medical devices
Council Directive of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (90/385/EEC)
Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices

controllers tend to escape from the responsibilities making the implementation of any law difficult (statement shared also by the expert N1), so the new responsibility scheme should address these problems considerably.

Expert H3 stated that the GDPR seems restricted in comparison to the US legislation from the point that the US legal system defines personal data as a property where the GDPR approaches it as a fundamental rights perspective (also noted by the Expert N1). The expert found this distinction counterproductive for the EU in developing AI technologies.

Experts H4, H5, and H6 referred to the problems presented in the scenario and stated that these were the exact problems currently exist in the application of the GDPR. Expert H6 also noted that the GDPR was very lately entered into the EU's legislation and without considering certain technologies like AI and blockchain, so this could raise some difficulties in the application.

Finally, Expert I1 and H5 made a general evaluation of the GDPR and said that the GDPR's derogations are very wide which would result in very different implementation in the 28 MS.

3.1.3. Risks Specific to the AI and HSR

"There is no human-human interaction anymore. Generally speaking, legislation regulates humans to human relationships. AI introduces a new type of relationship; human-machine relationship, or even more, machine-machine relationship, and this relationship is fake"

Sandra van Heukelom-Verhage (expert interviewed)

When we asked about the experts' opinions on the risks deriving from AI technologies from the data protection point of view, they all reported different than each other. Expert I1 reported that the use of a robot could be compared to using cars from the usual risks and accidents point of view. In this case, Expert I1 did not make a difference between robots with AI and cars or motorbikes. Expert I2 stated that data storage and hidden usage of the outcomes of algorithms together with such data to be sold to the other parties for any reason, including for political marketing, constitute the biggest risks (e.g., Cambridge Analytica case). Expert F2, similar to the Expert I2, noted that the third party disclosures are the biggest risk with the AI processing personal data.

Among those, the Expert N1's approach was regarding the technical complexity of the AI technologies which make it hard to foresee the consequences, to estimate what self-training algorithms were priory taught (whether the data carries some biases, shared view by the Expert N4), and therefore to estimate the outcomes (similar to the unpredictable by design concept). The expert pointed the problem with the explicability of such technologies (also shared view by the Expert N4), due to its high technical and connected nature (with the other technologies) which also makes it hard to implement the principles of transparency and accountability, even some of the rights given by the GDPR to the data subjects such as Right to be Forgotten[528]. According to the Expert, this complexity challenges assigning the responsibility and liability in a right way (therefore there should be a more interpretation and a standard liability scheme, as the expert stated). The expert thinks that the courts or the DPAs could generate such interpretations, based on scenarios like we presented. Finally, the expert pointed out data disclosure risks, e.g., the user of the robot discloses the other persons' data to other third parties.

Expert N2 referred to the risks deriving from the use of AI in public institutions and government. The expert referred to the text published by the Dutch Ministry of Justice reporting the risks and the guidelines to minimize these risks. According to the official report,[529] the transparency of the algorithms, verifiability of their outcomes, and legal protection against the ADM were the listed risks in the context of AI. The document further stated that the algorithms were not sufficiently addressed in the GDPR, therefore there is a need for specific safeguards[530] (within the specific legislation such as administrative law and consumer protections) to reduce these risks[531].

Expert N3 noted the risk of human dependence on the robot and the HRI manipulating the people to disclose more data as the biggest risks. The Expert stated that the robots should only follow the human orders and complete the tasks assigned by humans; business models (mostly followed and imposed by the companies in third-countries) should not prevail in this fact in name of profiting from these robots.

[528] The expert gave the example of blockchain technologies in which the data becomes a unit in a block to make it chain, basically, and it is not practicable to delete that unit from the entire blockchain.

[529] Brief van de Minister voor Rechtsbescherming Aan de Voorzitter van de Tweede Kamer der Staten-Generaal Den Haag, 8 oktober 2019 p.5.

Transparency risk recognized in the letter is almost the same as we identified in the Second chapter of this work. The Dutch Ministry of Justice raises a solution on how to ensure transparent information is provided to the data subjects. In this sense, "the clarity about the model or algorithm used, the procedures followed by the algorithm, the data sets used, including their quality and origin, and the variables and/or assessment criteria that are decisive for the outcome" could be some steps to take to ensure the transparency principle.

[530] Ibid., p.4.There are eight guarantees expressed in the Ministry's letter which are laid down as a result of expert opinions: Awareness of risks, explanation, data recognition, auditability, accountability, validation, testability, information to the public.

[531] Ibid., p.3.

Expert N5 stressed the problem with the possible risk of excluding people who cannot afford to have the means of technologies to access personal services. The Expert referred to a mobile application that collects notifications from the citizens regarding the particular services of the municipality (e.g., left trash on the street) which the notifications are then analyzed by the algorithm to assign a necessary task to the related department of the municipality. The Expert stated that not everybody may have the means of using such technology, so to use the application, to make their statements to the municipality. This may exclude them from a causal relationship with the authorities.

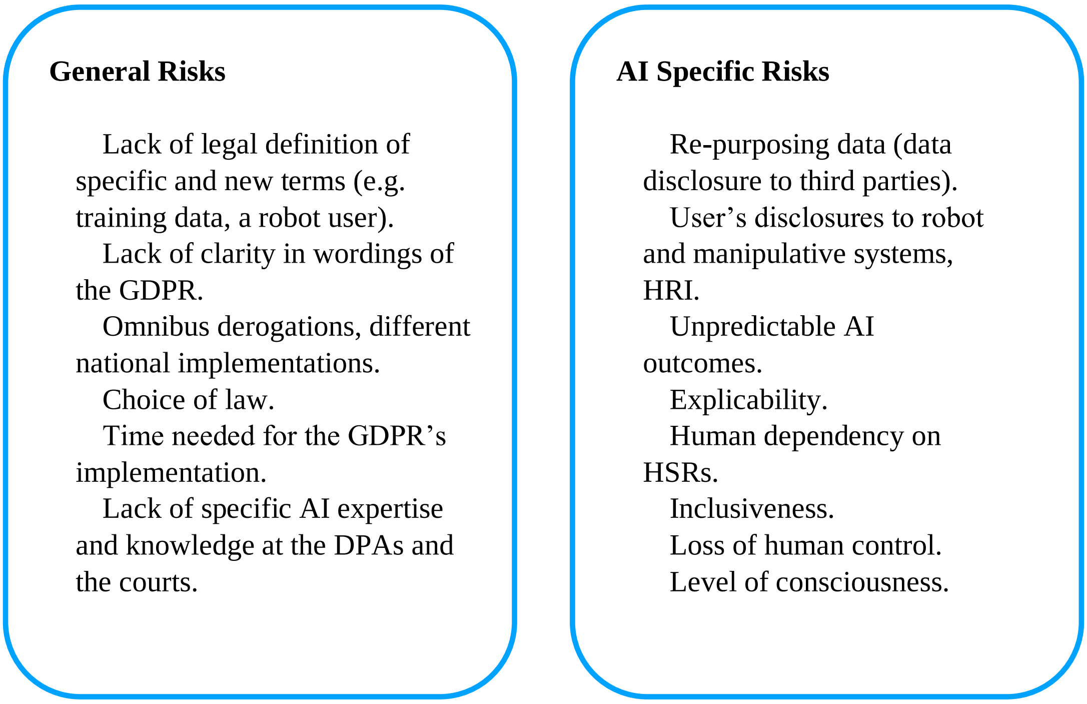
Expert H2 made a general risk statement with the AI technologies developing out of human control and limitations which then turn them to be evil for humans.

Expert H5 indicated that the biggest risk towards AI technologies is the level of consciousness which may lead AI to decide on removing the human being from the earth to protect the environment.

3.1.4. Summary

- Based on the expert feedback, the scenario presented in this work is valid and reliable. All the experts fully understood the scenario and the questions referred, and they accepted the scenario without serious criticism that may affect the reliability and validity of it. The experts like the scenario most because it multi-touches in several fields, such as social, legal, practical points, and the fact that it is not only futuristic but includes realistic elements. Some of the experts indicated that the method we chose is a good practice for lawmakers to foresee the possible loopholes in the GDPR.
- The experts sometimes reflected common problems, but also noted different ones regarding the application of the GDPR on AI technologies. Altogether those problems are, definitional problems (such as the definition of training data and social robots) in the current EU legislation, the lack of clarity in the wording of the GDPR (significant effect term in the Article 22), and the lack of practices and implementation which would come to force in a long time. One expert stated that the questions referred in connection with the scenario are already the real problems the expert also would point out.
- Some of the experts, without a significant difference between an expert from NSA or a law firm, stated that the GDPR is an obstacle for the companies to tackle with many consent papers proving their compliance with the rules identified in the GDPR.

- There are several risks identified by the experts regarding data protection in AI technologies. In general, bias, third party disclosures, and hacking were listed in the first case. AI-specific technological complexities and their effects on the applicability of the GDPR (from the transparency, accountability, right to explanation, liability, and R2BF point of view) were also stressed. From those, unpredictable outcomes and the difficulties to practice the principle of transparency were defined in this work, too. Sharing the other people's data (by the main user) with robots and the robot's possible manipulative effect on humans forcing them to share more personal data were both identified by some of the experts, as discussed in this dissertation. Below, Figure 8. illustrates these risks for an easier and better understanding of the reader.



General Risks

Lack of legal definition of specific and new terms (e.g. training data, a robot user).

Lack of clarity in wordings of the GDPR.

Omnibus derogations, different national implementations.

Choice of law.

Time needed for the GDPR's implementation.

Lack of specific AI expertise and knowledge at the DPAs and the courts.

AI Specific Risks

Re-purposing data (data disclosure to third parties).

User's disclosures to robot and manipulative systems, HRI.

Unpredictable AI outcomes.

Explicability.

Human dependency on HSRs.

Inclusiveness.

Loss of human control.

Level of consciousness.

Figure 8. Risks regarding AI technologies and implementation of the GDPR.

- We noted that, although there exist some EU directives regulating and defining very specific technologies, the definition of a social robot is not referred specifically in any of them. In other words, there is no definition of a social robot made in the EU legal texts.

- Some of the experts stated that either the GDPR's derogations, the national interpretations, or a lack of knowledge on AI technologies (judges, lawyers, and the DPS officials) would result in different implementations of the GDPR in the EU.

- Finally, as we also observed during our research, and as the Experts F2 and H3 verified, the bigger problem with the application of the GDPR that is the visible tendency in most of the National DPA’s waiting for the EU *to do something*, instead of generating a GDPR guidance for the AI industry (there are some for the public institutions, but not in all MS). In the course of the analysis we were making, we realized that the Dutch and Finnish DPAs are more actively preparing agendas and working on the AI and ADM, while there is no such preparation observed in the Italian and Hungarian DPAs.

3.2. Evaluation of the GDPR Specific Questions

In this section, we will present the outcomes of the experts' opinions on the specific questions related to the GDPR and AI technologies. The aim of those questions was to investigate the practicability of the GDPR and was to find out whether there would be different opinions of the experts from different countries.

3.2.1. The Household Exemption, the Joint Data Controllership, and the Liability Questions

First of all, there is no doubt that the first and the utmost controller is the Company, so we are not questioning whether the Company would claim the exemption, therefore anyway exempted from being a data controller. We are aware of the reality that it is and it will always be the legal persons responsible for their wrongful acts or for their unforeseeable acts in case they breach the GDPR. As one of the opponents to this dissertation pointed out, the GDPR explicitly refers to the data controllers to take the necessary actions, such as conducting a DPIA or implementing the data minimisation principle, to proactively avoid harms and other unwanted consequences of data processing. The responsibility of a natural person as a data controller has a small space in the EU data protection legislation, in theory. However, as the below expert views will reflect, there is no common approach to the responsibility of the natural persons in the frame of the GDPR’s application which raises questions about the uniform applicability of the GPDR.

We noted divergent expert views on Julia’s possible controllership and on interpreting the household exemption, not only among the countries but also within the same country. During the interviews, besides the question for Julia to be assigned a joint controllership, possible separate data controllership for Julia was also discussed. Experts’ views are sharply divided into two groups:

- Julia absolutely is not a joint controller and is not a separate controller. Robinsan's company and the other persons referred to in Question 6 (related to identifying the other persons in the scenario) are the absolute controllers and liable persons.
- Julia might be a joint controller but absolutely is a separate data controller based on the scenario, therefore she should bear a certain level of liability.

The household exemption is applicable	The household exemption is not applicable
Experts I1, H1, H4, N4	Experts F1, F2, N1, N3, N4, H2, H3, H4, H5, H6

Table 3. Experts' opinions on natural person's joint data controllership.

There are several reasons noted behind the experts' statements. According to Expert I1, using Robinsan is not different from using a personal agenda since the use of it was not intended to be in the public space, but for purely personal purposes. Just like a possible risk for the agenda causing data leak, the user of Robinsan would not be responsible for any data leak. The expert also said that even the company could claim that Robinsan's use falls under the scope of household exemption, and it should not be assigned any liability in the frame of the GDPR (but probably does have under the consumer or competition law). Similar to that, Expert H1 stated that the case would fall under the household exemption for Julia since the Expert compared the use of social media by natural persons who are usually not held liable for using it, as also indicated in Recital 18. The Experts H1 and H4's joint opinion is, as we observed, regarding the civil liability of Julia (she puts the input and should be aware of the consequences) to inform her son and take care of the well-functioning of the robot. This means, that Julia does not have any obligations as a data controller, but may have under the civil law, such as to inform people entering her home about the existence of and the risks of data processing activities done by Robinsan.

Expert H2 thinks that there is a possibility for Julia to be considered as a data controller, but certainly not as a joint controller. Expert H3 stated if Julia chooses the settings of Robinsan for her wishes, there could be a joint controllership, but it should be assessed carefully on a case by case basis.

Expert H5 identified two types of data processing activities based on our scenario: one of them is the data processing activity based on a relationship between Robinsan and Julia, and the other one is the Company's data processing activities. If Julia has a connection between Robinsan and her public social media accounts where she shares the outcomes of Robinsan's data processing activities, such as her therapy results, or other data including other persons' data, then she could be identified as a joint data controller. Regarding the Company's data processing activity, it should be made clear that what the Company doing was only putting the hardware, or collecting data based on certain means and purposes, according to the expert. According to the expert's opinion, the Company would not be a data controller if it only ensured the hardware equipment necessary for operating Robinsan. In case Julia is a data controller or joint data controller, then she is obliged to ensure all the requirements of Article 7 of the GDPR to use Robinsan at home, the expert added.

Expert F1 clearly stated that Robinsan's data processing activities do not fall under the household exemption, and Julia could be held liable if she starts streaming her home-life with the other people or if she shares other people's data with Robinsan. We think that during the HRI there is a high possibility for Julia to disclose other people's data to Robinsan as long as she lives and becomes dependent on Robinsan. For example, she could easily share her memories or feelings about other persons including some personal aspects of those people's life. Specific to our case, the Expert stated that Julia would not be a controller since, first, she could not be a controller of her own data, and second, her son was not happy with the outcome of the robot, not with his mother. The Expert noted that when there is a health-care service given via any technology at home, other people entering that home must be protected ("the device should be kept in a box", as the Expert stated). According to the Expert, it should be absolutely the Company that should inform the users about the usage and risks of such technologies. On the other hand, the Expert gave an example of the persons creating Facebook groups for promoting solidarity events without considering the risks before other people's data protection rights. To our understanding, there is a sharp difference whether Julia uses his son's data somewhere else (publishing or disclosing to a public or other legal persons) or keeps it for her own personal purposes. We then realized that we could have inserted an extra event in the scenario, indicating Julia's automatic data sharing activity with the help of Robinsan on her social media account, because this would certainly make her a joint controller.

Expert F1 said that if Julia disclosed her son's situation to a doctor, this would automatically make her a data controller. On the other hand, Expert H5 stated the opposite, that even in that case Julia would not be considered as a joint controller. It is important to note that both experts have gained experiences working as an expert in a DPA.

Experts F2, N3, and H2 do not give any chance for Julia to be considered as a joint or data controller by the DPAs and courts. They are in favor of the full liability of the Company. Expert F2 especially stated some worries on the CJEU's broader interpretation of the data controller after the GDPR entered into force. The Expert also stated that the bar for a natural person to be counted as a controller is very high ("should we informed everybody coming our home about the smart lightning which turns on and off based on a weight of persons?" the expert noted).

Expert N1 thinks that Julia is a joint controller based on our scenario and the case does not fall under the household exemption for her. The exemption is very strictly applied for a small number of cases, as the expert stated. The reason why the Expert considered Julia to be a joint data controller is the fact that she actively was putting several specific data in Robinsan and make it work by learning directly from Julia. She purely controls the robot, according to the expert. Julia should have fulfilled at least the informing obligation, in this case, as it is clear that Julia cannot perform data correction and data deletion activities within the robot's system. Expert N4 gave an opposite view; the algorithm was designed by the Company even if Julia teaches the robot what data to collect and how to evaluate it, and even if Robinsan could find new means and purposes for data processing, Julia cannot be assigned any liability.

Unlikely the Expert N1, the Expert N4 indicated that Julia is an end-user, and she only puts data to develop the machine. She is not sharing the same purposes as the Company, but she might be a separate controller because of her personal purposes, therefore she must have informed her son about Robinsan's functionality.

The most different opinion among the experts on Julia's liability was delivered by the Expert H6 who made a general evaluation on the applicability of law on non-human beings and stated that it will be always human who is the main responsible behind any type of technology. Specific to our scenario, the expert noted that both Julia and the Company are jointly responsible, but Julia bears most of the responsibility since she is operating and using Robinsan although Robinsan seems like making the decisions (it is the output what the expert refers). Such operating brings a heavy risk for the data inside Robinsan's system, because according to the expert, "It is the technology we bear the most risk. Information is the risk.

All the words we do speak will not be remembered unless it is recorded somewhere electronically which makes it unforgettable".

Expert N3 stated that the Expert would never think about Julia's data controllership, so it is an interesting aspect. Especially the companies trying to escape responsibilities would try blaming the users in this way. This complicates not only defining the responsibilities of natural persons, but a clear distribution of liabilities among the government, and also small companies. Finally, the expert said that if Julia was given all proper information on the "hazards" of Robinsan, then she could be held liable for not following the rule.

There is only one expert who did not give a clear answer to this question and stated that more details are needed for a clearer evaluation. The expert was looking for more details on the person deciding the means and purposes of the data processing activity. Still, the Expert stated that the case would not fall under the household exemption from the Company's point of view[532].

Although it is not referred as a research question in this work, we asked some of the experts' opinion on the electronic personality of AI systems or robot's liability, but except the Expert H5, none of the experts gave even a small chance for the EU lawmaker introducing such a new concept in the legislation. Expert H5 raised the situation in which Robinsan could work offline (no data is transmitted to a company) and can make its own decisions that cannot be predicted by a human. In such a situation, the expert thinks that there could be a concept for artificial personality for a robot, but this is yet far from the current legal framework.

According to our scenario and the question on the household exemption, there is a probability for natural persons as users of personal robots at home to be assigned a controllership and therefore to be held liable for their actions related to data processing activities. Table 4. shows the diversified opinions of the experts in different countries with this sense. In Italy and Finland (although the case's details would change the experts' opinion in Finland, as the experts clearly stated), the possibility for a natural person to be a data controller is almost impossible. In the Netherlands, while the Dutch DPA would share the Italian expert's opinion, some of the law offices in the Netherlands would assign a controllership to a natural person. In Hungary, there might be even more diversified approaches; experts independently from their affiliations would interpret the case differently; either within the Hungarian DPA or among the lawyers there would be different

[532] Some of the experts were initially interpreting the case as we were asking for the validity of exemption for the Company. We clarified the situation by giving more explanation during the interview.

approaches to the question. Especially, some of the lawyers indicated that they would definitely try to use this question before the court if there were to defend the Company in a referred case. Either under the GDPR or the civil law, Julia should inform people entering her home about Robinsan. Indeed, to do this, first Julia needs to entirely know what Robinsan can do and can raise as a risk. Referring back to the scenario, Julia represents the average data subject who does not pay much attention to the information presented by the data controller; and the Company represents the average data controller who provides some technical and long-lasting information.

Data controllers matrix	Julia is/might be a controller	Julia is not a controller
Joint controller	Expert N1, N3, H3, H5, H6	Expert I1, F1, F2, H1, H4, N5, N6
Data controller	Expert N4, H2, H5, H6	(Not Applicable)

Table 4. Data controllers matrix.

3.2.2 Sharing the Responsibilities: Article 26 of the GDPR

As it was clear under the previous analysis, there is a probability for a natural person to switch her role from data subject to a data controller, and even to a joint data controller. In this case, Article 26 of the GDPR provides a legal basis for joint controllers to share their responsibilities deriving from data controllership based on a contract. We asked those experts who assigned a certain joint controllership to Julia whether and how contractual relations between Julia and the Company could be established in this sense. Most of the experts indicated that there is a need for establishing rules on how to make joint controllership contracts as referred to in Article 26 of the GDPR. The question on how to make a valid contract with the companies from third countries (such as the US-based companies) is a difficult one, as the Expert N6 stated. We think that such contracts often fall under the consumer law (which might have a national application since there exist only

Directives[533] in this sense) and which law to apply is another question, as the experts stated. Expert H6 thinks that regulating the relationship between Julia and the Company is what the law serves in regulating people's life and contracts are the most flexible tool to regulate this relationship. The Expert believes that writing down a valid joint controllership contract between Julia and the Company is a lawyers' duty since they know the law and how to practice it. Expert N1 already indicated that where the expert works, they already provide legal assistance for data controllers to identify the joint controllers and conclude contracts with them (although none of them is a natural person, yet).

We asked those experts who indicated that Julia could not be considered as a joint data controller to make some statements on Article 26 to gather their general opinions. Experts F2, I2, and H4 said that there shall never be a contractual relationship between a natural and legal person since it creates imbalanced power situations on the natural persons. A possible joint data controllership agreement between the companies should list all the responsibilities and obligations, liabilities, and the responsible persons with a clear division between all and written in the contract, according to the Expert. Expert N1 said that ensuring the existence of the joint controllership is the main data controller's duty, so it should establish the contractual relationship with the joint controller. Expert H4 noted that two companies could sign a joint controllership agreement since they share the same level in terms of, for example, implementing the security safeguards, but this is not a valid issue between Julia and the Company. In this case, the Expert said that even the Company could impose certain conditions to ensure secure data processing for Robinsan, it will always be the Company holding the obligations and responsibilities, without sharing with Julia. Some experts stated that the NSAs are exactly there to not to put the natural person in an asymmetric power situation[534].

Our position is that, if there is a clear joint controllership relationship between a robot user and the company providing the robot, there could be a contractual relationship, but the only responsibility of the user should be to "know how to use and how to not to use" the robot. We will explain this statement in the Recommendations section.

[533] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance

[534] Article 57, 1 (e) of the GDPR states that: "(NSA) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end".

3.2.2.1 Responsibilities of the User

All the experts answered this question (8 experts) stated that there is no difference between natural and legal persons in the GDPR in terms of their obligations and responsibilities as a data controller. Particular to our scenario, there are different opinions noted by the experts on Julia’s responsibilities. Expert F1 stated that natural persons’ responsibilities are equal to the legal persons and depending on a case, Julia should even conduct a DPIA. For this reason, Expert N1 said that there is a need for more interpretation in this sense and the expert’s opinion is that humans and machines could work together on fulfilling these responsibilities (also one of our recommendations). Expert H1 noted that the obligations of Julia may not derive from the GDPR, but from the consumer law which puts the responsibility on the users to fully understand the product they use.

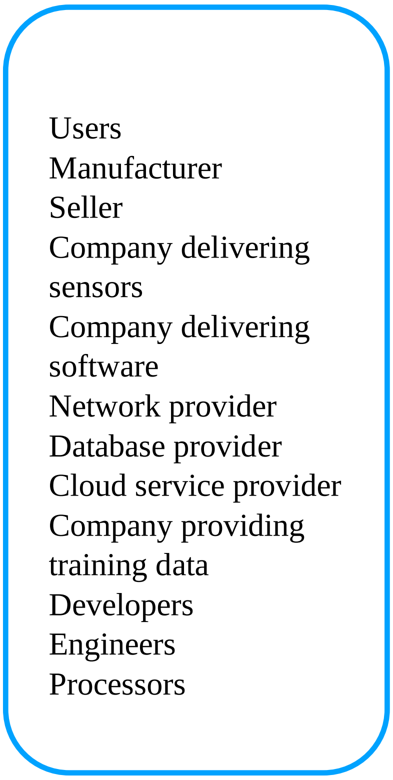
Expert H6 stated that since the user is the decision-maker on the use of this technology, she should ensure the safe and right operation of the robot together with fulfilling her informing obligations.

Expert H2 made a general comment on the question and stated that the GDPR mistakenly did not consider the size and impact of the businesses in terms of sharing the responsibilities, and the same goes for the difference between natural and legal persons. Expert N5 made the same statement and agreed with the Expert N1 on the necessity of generating more interpretation. Expert H3 noted that from the risks point of view, Julia and the Company should not share the same responsibilities and an NSA would never investigate the natural person in this sense. However, the expert we interviewed from the Hungarian NSA said that Julia must conduct, for example, DPIA if she is considered as a data controller which makes her a subject to investigation by the NSA.

Our position to this question is that Julia cannot alone guarantee other people to exercise their rights given under the GDPR, however, as the case law we analyzed under the “Preliminary analysis of the scenario” title, she must at least fulfill her informing obligation on Robinsan and on the rights that data subjects have.

3.2.2.2. Other controllers and processors in the Scenario

Although we restricted our scenario among three main players (the Company, Julia, and her son), we asked the experts' opinion on the other possible persons involved in Robinsan's data processing activities to see how could the scenario be much more complicated.



Users
Manufacturer
Seller
Company delivering sensors
Company delivering software
Network provider
Database provider
Cloud service provider
Company providing training data
Developers
Engineers
Processors

Figure 9. Possible data controllers in HSR system

All the experts more or less referred to the same possible actors as part of the data processing/controllership chain related to the services Robinsan offers. Expert I2 stated that in real life, there are a few probabilities on the Company providing Robinsan is alone; there will be more than one company providing Robinsan. Hardware provider (e.g., company delivering the sensors), software provider, data service (e.g., network provider or company providing training data) and database provider will all take a part in Robinsan's services in the real-life application (Experts N3, H4, and F2). Manufacturers, developers, engineers, and all the users are also the persons involving Robinsan's operation. Expert H3 made a special note regarding authorization which may raise the number of users accessing Robinsan's services.

3.2.3. Defense of the Company, Defense of the User

Since we built our scenario on an assumption that the Company's behavior blaming Julia to get rid of some of its responsibilities, we asked the experts how would they defend the Company against Julia and her son, if there was to be a court hearing afterward. The same question was asked in the situation of defending Julia and her son against the Company.

Almost all the experts said that they would try to blame Julia for not using the robot properly, and further put emphasis on the Company presented all the related information to her if they were to defend the Company. If they were to defend Julia and her son, almost all the experts stated that they would blame the Company for not presenting clear information on Robinsan's use and the possible risks for Julia and her son. We observed that it would significantly differ, if a lawyer takes the case to defend the Company and if an expert in the NSA is responsible for defending Julia and her son. We are sure now when such a case will be real in the future, lawyers defending the robotics companies will try to put the responsibility and liability on the HSR users.

Expert F1 illustrated the situation with the cigarette companies who just provide the cigarette and leaving the responsibility to smoke or not to smoke to the people. The Expert said that the administrative court in Finland would not accept such a defense, but the criminal court would consider as a valid argument. Expert F2 stated that the Expert would collect all the valid consent statements and bring before the court against Julia, but the Expert does not think that it would be acceptable by the judge. The Expert also stated that AI and ethics courses should be given to avoid such complicated issues since it would make even more complications if such a case is referred to a court.

Expert H4 also would try to blame Julia, but then stated that the Hungarian NSA probably would not accept this claim in the first place even before referring the case to a national court. However, if the Expert was in a position to defend the Company, would refer to Article 29 WP's transparency rules which the Company was assumed fully complied with in accordance, and Julia and her son should not be surprised about Robinsan's data processing in return offering those services. On the other hand, the Expert would claim that the Company misused the instructions related to Robinsan and did not fully make Julia and her son aware of the risks it could raise.

Expert H1 would refer to the Basic Law of Hungary Article O starting with "Everyone shall be responsible for him or herself," if the Expert was to defend the Company. The Expert would claim that Julia had to be aware that Robinsan and she together start a new life; Robinsan is a new entity with its decision-making capabilities (even if at a restricted level) to serve her. If the Company presents sufficient documents to the court, it would be enough to save the Company, according to the Expert. The unpredictably of Robinsan would not be persuaded, according to the Expert, but would worth trying. If the Expert H1 was to defend Julia, would surely refer to the design of Robinsan which was not considered in line with the DPbD rules, letting the system disclose information about people to others.

Expert H5 would point personal use of Robinsan and claim that purposes of use of Robinsan are identified by Julia (e.g., ordering the medicines) who should bear the responsibility, in this case. The Expert, on the other hand, would defend Julia by stating that the information provided by the Company was not transparent, even Julia's son did not understand the information, and the Company did not offer testing opportunity before the purchase. The last point is already one of the solutions referred to in the Recommendation part of this work. The Expert also would claim that the Company did not implement the data minimization rule by collecting all data without a border and irrelevant to its main services (cheering up the user, not making her sad with the information on her son's possible drug addiction).

Expert H6 said that the Company would use all means of training to close the doors to any of its liability. This is already one of our main solutions offered at the end of this work.

3.2.3. Consent and Purpose Limitation

One of the novel parts of this work is the investigation of consent as a legal basis which probably the data controllers operating personal robot would try to use. In the theoretical part, we assumed that ensuring the validity of the consent of a HSR user is very difficult, if not impossible. Almost all the experts we interviewed shared our position in this sense and stated that purpose limitation and transparency of algorithms in robotic brains are some of the most difficult issues to ensure from the data protection point of view. They also think that consent alone is never enough for such 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.

Expert I1 clearly stated that the Robinsan's system should be constrained in a way that only the expected purposes should be operating during the actual serving to Julia, but the Expert also would welcome to receive personal suggestions by Robinsan to make the Expert's life easy (e.g., the robot could “guess” the users eating habits from the goods in the fridge, and suggest some restaurants in line with it). In our view, this is easy to assume purpose, but we are not sure whether the data controller could foresee the other possible purposes from the beginning without the actual use. Expert I1 added that what we stated is true, but at least general information on the capabilities of the robot could be drawn and presented to the user. The user should be informed very clearly from the beginning, as the Expert noted, and as we also stated before.

Expert I2 said that consent in this scenario is not a sufficient practice, but it would surely be the legal basis chosen by the robot companies in the future. Prior consultation with the NSA is needed (if the DPIA was carried out in line with the Article 36 of the GDPR and the high-risks found are not tend to be mitigated with the controllers’ actual safeguards) before placing these devices to the market, as the Expert thinks and, it is not possible to regulate them before there is actual use.

We think that this might be a wrong approach if one of the aims of the GDPR is to prevent data breaches proactively.

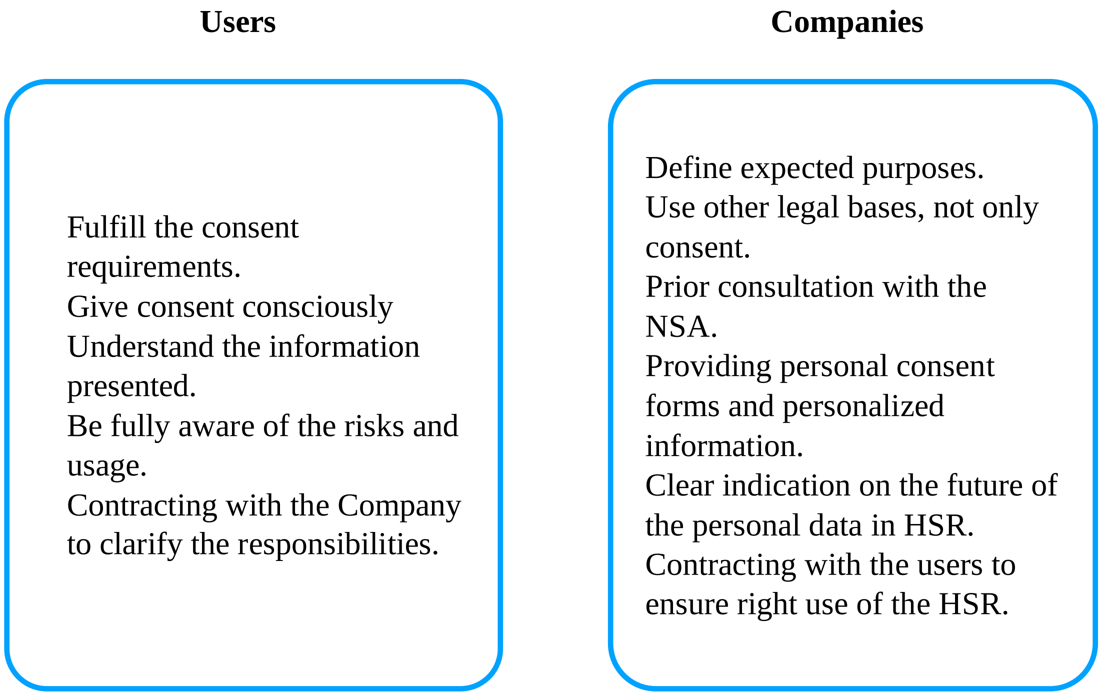
Expert F1 evaluated the consent in the scenario as it is similar to what the American companies (still) do which is not acceptable in Europe. The Expert said that some American companies do perform some informative activities to their users before introducing them their services (we then immediately stated and the Expert agreed that few companies are doing the right thing in such a way based on their initiative in order not to lose their clients’ trust) because their business logic is different; for example, they work for public institutions. The Expert pointed out a very important problem related to consent in the medical sector where a patient is under stress when giving consen**t,** otherwise, the patient’s accession to the medical services may not be possible. From our scenario’s point of view, the Expert questioned whether Robinsan is operating for offering treatment to Julia or for processing her data since this would change the interpretation from the core.

Expert F2 noted that obtaining consent is the pure duty of the company (so Julia should not obtain anyone’s consent), but how the company could do is a difficult question since using such a robot may have multi-ways in 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, not a generic one**.** While the Expert believes that ensuring valid consent is a fiction and the data controllers in Finland are not aware of how invalidly they obtain it, the Expert would not recommend data controllers to use consent as a legal basis, but the legitimate interest rule (later, two more experts stated the same). Finally, the Expert said that consent in the scenario was not valid, because the context and the consequences of usage were not clearly stated to the user before.

Expert N1 thinks that the company should have obtained the consent of Julia and her son, but it was clear for the Expert that her son was under power imbalance since he had to give his consent for contributing her mother’s treatment offered by Robinsan (Expert H2 made a very similar statement on the consent misleading Julia negatively affecting her informational self-determination). In this sense, the Expert thinks that Julia also should have informed people entering her home about Robinsan, but first, she must have known every aspect of it, and this should not be thought of any interruption of people’s daily lives. The Expert stated that people should separate much more time understanding how the robot or any technology they involve with works which we completely agree with. Users should check their knowledge on these technologies from time to time, according to the Expert. Similar statements were shared also by the Expert H1 in a way that Julia must have been aware of the possible risks coming with Robinsan (the expert gave the example of a toaster “if you do not switch it off, you could burn the house”).

Expert N2 made a general evaluation of the wrong practices in obtaining consent and said that companies always use data for their profit without disclosing this fact to their clients. The Expert further placed the following question: “How do they use data is never clear neither to the users as public institutions or to the natural persons?”.

Expert H1 thinks that Julia and the Company should have concluded a contract also certifying her consent ensuring the right use of Robinsan.



Users

Fulfill the consent requirements.
Give consent consciously
Understand the information presented.
Be fully aware of the risks and usage.
Contracting with the Company to clarify the responsibilities.

Companies

Define expected purposes.
Use other legal bases, not only consent.
Prior consultation with the NSA.
Providing personal consent forms and personalized information.
Clear indication on the future of the personal data in HSR.
Contracting with the users to ensure right use of the HSR.

Figure 10. Experts' opinions on consent and purpose limitation requirements

Expert H2 noted that even if there is no crystal clear legal basis for operating such robots, in the beginning, it could derive later, but consent should never be alone a legal basis.

Expert H3 referred to three ways of strengthening valid consent for the data controllers like the Company in our scenario: delivering visual, textual, and oral information which all of them should be used at the same time. Only then the consent would be valid, according to the Expert.

Expert H4 does not think that Julia's son's consent should be obtained, but Julia's consent should be taken in a paper based-signed form prepared in line with the related Hungarian legislation. The Expert further stated that the Expert would use Article 9 point 2/h of the GDPR[535] as a legal basis for operating Robinsan's healthcare support services. Expert H4 also stated that providing information on the operative aspects of the algorithm may cause disclosure of the Company's trade secret, therefore the Company may refrain from

[535] This Article is one of those derogations in the GDPR leaving the Union or MS law, or to a contract to regulate data processing activity for the purpose of "preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health" with the condition of ensuring the secrecy provisions under the Union or MS law, or to national competent bodies.This rule could overarch the consent as a legal basis and may cause different implementations EU-wide.

delivering some of the information to Julia, and deciding which information may fall or not under the trade secret would be defined by the Company.

Expert H5 strongly believes that Julia must have obtained other people's consent when they entered her home without an exception to Article 13 of the GDPR or she should have switched Robinsan off.

Expert N5 stated that data collection by Robinsan should be based on consent and the GDPR's consent rules are very clear and strong, but in practice, there are too many consent statements in real life making it hard to ensure right and specific information was given to the users.

Expert F1, N1, and N3 stated that it is true that there is no rule for ensuring the understandability of the information data controllers provides to the data subjects in the GDPR. There are other standards and guidelines according to the experts, to be used for that, but we believe that these are only under the data controllers' initiative to follow or not.

3.2.4. Providing Information to the Certain User Groups

All the experts without an exception stated that if the user of a robot is an elder person, the company should provide different information. Their health conditions (Expert F2), culture, age, education, (Expert I2), and their vulnerability (Expert H1) must be taken into account when providing information. Different groups need different attention and treatment from the awareness-raising point of view, as the Expert N1 stated since they are not raised with these technologies, as the Expert N5 completed this statement. However, the experts noted that this rule is not directly inserted in the GDPR, and some of the experts stated that such a rule could be found in the consumer protection law. Expert N5 also said that the guidelines generated by the different NSAs and the EDPS, EDPB/Article 29 WP highly affect the NSAs decisions in this sense, so the guidelines should be taken into account by the data controller when preparing information to their users from different user groups.

Only the Expert F1 said that the GDPR should not discriminate against the data subjects based on their age, but about delivering information, it may depend on a case by case analysis.

Expert H5 stated that Julia already is a vulnerable person and should be given specific and personal information by the data controller.

Lack of information together with manipulatively designed robots would certainly cause data subjects to disclose more information to robots. 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 stated that the GDPR should not restrict companies in this sense. Expert H1 stated that it might be even a positive aspect of the robot to encourage people to share their lives with it since there are many lonely and desperate people in Europe, but they must be aware of the consequences of their interaction with the robot. The expert gave the example of smoking which the law failed to prevent people from and stated that law could not always prevent people from making a mistake. 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. The expert further thinks that it should be researched in psychology before those robots become more common in society. Expert N6 thinks that this question is related to ethics, besides consumer protection, and the expert stated that it is a very interesting question to be thought on, further.

3.2.5. Right to Explanation is a Reactive Right

All the experts we interviewed stated that there is a right to explanation placed in the GDPR although not explicitly stated, and it is an ex-post right complimenting the other ex-ante rights, such as the right to be informed before processing started or the general principles such as fairness and transparency (Experts F2 and N5). Expert H5 stated that exercising the right to explanation is for just a starting point for data subjects to look for a possible remedy and only with an explanation from the Company, Julia or her son could apply to a DPA or a court.

Expert I1 pointed out the intended "why and because relationship" with the right to explanation and stated that it could be the engineer or even the robot who could explain. While exercising this right, the data subject should receive an answer to the following question: "Is it the conclusion what I want?", the expert continued, and said that this is more related to the Consumer Law than the GDPR.

Although it might be difficult to change the outcome of the algorithm, data subjects still should know what should they have done for the algorithm not to generate this outcome, as the Expert N1 noted. The expert also drew our attention to the difficulty of making the algorithms forget data or a set of data since they are all interconnected in the AI system.

Expert N3 gave the example of judges who first make the decision and then explain why did they decide so. The expert believes that the right to explanation at least ensures how the system could be designed after the data subject’s request. The expert also noted that the data controllers could generate explanations for everyone to understand how their algorithms work simply, but they do not do so in practice.

Expert N4 said that it is not acceptable if the decision-makers (based on algorithmic assessments) state that they do not know the rules of the algorithm they work with, anymore. It is true that once Robinsan generated an outcome that might be even highly likely to be true it is difficult to make afterward explanations.

Expert H3 thinks that the robots in such should not be given a chance to make a decision which should always be under the controller of the data subject, and data controllers should block the unwanted decisions immediately.

Expert N4 indicated that there is yet no case brought to any jurisdiction and the CJEU on algorithmic explanations, so we do not know how the court(s) will interpret such an issue, hence, we do not have any guideline on right to explanation. The expert thinks that humans always could justify her decisions, but this might not be as easy for the algorithms.

Our observation from the experts’ opinions on the right to explanation is that there is no understanding of how it shall be interpreted if they receive a case and when they receive a case, they do not have any resource to benefit from, so they would make their interpretations. This, alone itself, could cause many different GDPR practices in the future.

3.2.6. Summary

- Expert feedbacks on the responsibilities of the user of HSR approve that natural persons should have a certain level of understanding of the technology they use. Our scenario and the questions related to consent proved that consent in practice does not work (agreed by Expert F1, F2, N2, N3, H5, H6, and I1). There should be more activities on raising the awareness of the users not only in AI-specific but technology in general. Since the main data controller also could claim Julia to obtain her son and other people’s consent, it is an ultimate issue to make her fully understand Robinsan’s operation.
- On the other hand, we ensure the data controllers’ possible claim (or blame) on data subjects (or users at public institutions) to fail to understand and properly using the robot caused other person's’ privacy infringements. We also proved, that ensuring the

understandability of the information data controllers provide, together with safe operation rules, are the certain responsibilities of the data controllers.

- Although there are not data subject groups identified in the GDPR except a general classification of the children and the others, data controllers must ensure the information they provide to be in line with their user groups' needs, such as the elders. This necessity may not derive from a specific Article to be found in the GDPR, but from the fairness and transparency principles as two general rules. Data controllers must design their information based on the information needs of these groups.

- Proactivity should never be underestimated even if we are referring to the EU's slow pace in regulating AI and robotics sectors. During our interviews, we identified the Netherlands and Finland as have been preparing regulation of ADM and AI, and have been consistently working with related ministries and NSAs to make it happen. We did not identify such a preparation in Hungary and Italy. If there will be no common approach in the regulation of AI technologies in the EU, we should be ready for different applications which then will bring up a possible AI Regulation taking some years to enforce. By this time, some of the MS and the third countries would already be speeded up with the use of AI technologies as the others would just start. If this happens, we neither can truly expect a uniform application of the GDPR nor the EU to become an AI leader in the world.

- People should spend time understanding the technology they interact with and they should be encouraged to do so, if not obliged by law. We believe that who gains (financial, personal data, time, reputation, etc.) most from HSR must fulfill their informing obligation towards the other people. We share the Expert N1's statement who said that big tech companies must effort more because they gain a lot. We agree with both statements and will below draw our solutions based on that.

- We think that the classification of these robots in the legislation is the key factor in deciding how to interpret the possible legal cases in the future. However, it should explicitly bear in mind, that whatever legislation these robots will be regulated in, data protection will always be the main issue, therefore data protection rules must be dictated within any specific legislation regulating AI.

VII. Conclusions and Recommendations

1. Conclusion

In this work, we used a scenario and interview method to test our hypotheses deriving from comprehensive literature analysis and the case law analysis on the applicability of the GDPR on HSR. We proved that there are several practical problems with the consent rule; people do not read the privacy statements or do not understand those statements even if they read. Besides, they might not always be conscious about the possible consequences of AI technologies, especially, HSR. They may share other people's data with robots or may cause disclosure of other people's data to the robots. They might also not be aware of the fact that they may share some responsibilities and liabilities for doing so. Furthermore, data controllers of HSRs do not always keen on presenting fully understandable information to their users on the usage and risks of HSR.

Technical aspects of AI technologies make it hard for the data controllers to fully comply with the GDPR. Their unpredictable data collection and processing nature 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 may generate unpredictable outcomes, but as long as they fall outside of the purpose of the AI system, data controllers must ignore them and not display them 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 stopped by doing so since trust may increase the level of user's treatment. Eligible safeguards specific to this technology should be introduced in application.

The GDPR fully covers and gives a comprehensive legal framework for personal data protection issues arising in the AI era. However, more interpretation and guidelines are needed to reach a uniform application. For example, the concept of meaningful information and intelligible form should be interpreted specific to AI technologies. Our analysis showed that there are either different opinions on the questions referred, even though they represent the same country, or there is a full agreement on an issue raised. The right to explanation in the GDPR is reactive and there is no common understanding on how the explanations on ADM should be formed and delivered. Finally, there is a probability for the natural persons using HSR to be held liable under the GPDR. After this summary, we would like to present the whole conclusion in the table below. As a result of our research, it is safe to state that we would have a very complicated case with HSR and their data processing activities within the purpose of serving their users. The below figure should present this complexity and it should be read in connection with the other figures presented in the analysis part.

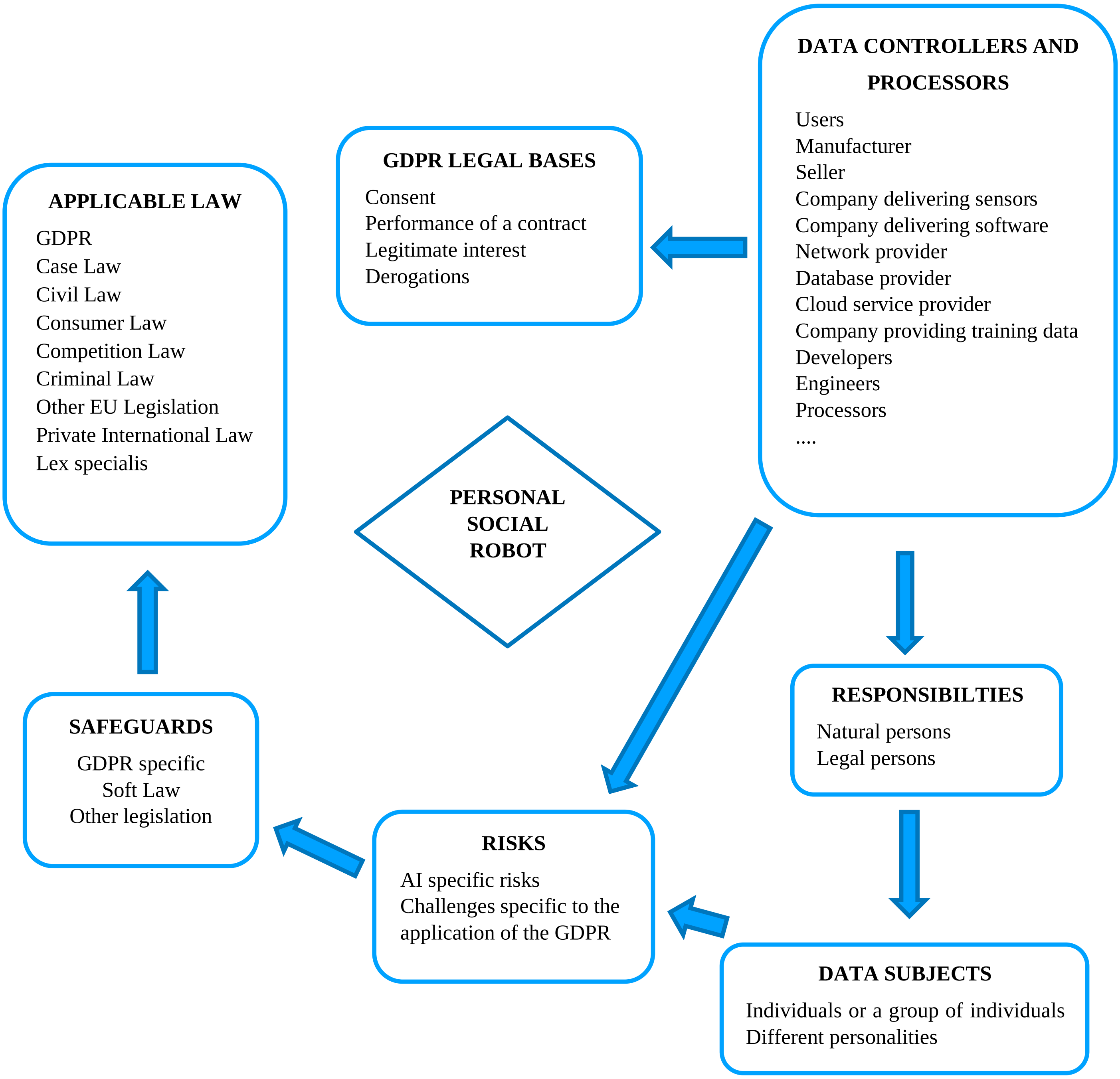


Figure 11. HSR and the GDPR

Within a 20 years or less, personal social robots will be introduced at households raising a complex relationship among the actors.

As it could be observed, the Solutions and Safeguards figure was left empty and was not explained before. Following, we wish to fulfill that and deliver our solutions and recommendations to the specific groups possibly involving AI technologies.

2. Recommendations

2.1. For Developers and Data Controllers

- Our analysis showed that the first and the biggest responsibility is on the shoulders of the data controllers. In this case, we propose a compulsory user education and training program to be prepared by them 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 interpreted with the users based on their person-specific case. Data controllers can engage users in the development and testing phase of the robot, or in the course of conducting the DPIA as suggested by Article 29 WP's DPIA opinion in line with the Article 35 (9) of the GDPR[536]. Pieces of training must be set by the level of user's understanding and their understanding must be verified and proved. We propose obligatory lifelong training programs for the people using AI systems to be able to catch any new developments within the system. The main controller should provide these programs by involving some informative presentations for the other possible data subjects, mainly to the family members of the main user. All training must be provided free of charge. Training should be delivered in a personalized way and the implementing of specific ML techniques for creating user-specific training content could be time and cost-efficient[537]. This way, full user control on the AI system could be ensured.
- An entire and a comprehensive internal training program for the company (the main data controller) could help to raise the awareness of its own staff.

[536] Article 29 WP, 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, p. 15. Art. 35 (9) of the 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.

[537] 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. Conti and Passarella's work could be a starting point to design such robots. See, Conti and Passarella, 2018.

- The second solution we propose is to ensure the validity and understandability of the information thee data controllers deliver to the users. We already noted before, that the information prepared for the users should be specific to their personal conditions (age, gender, education, etc.) and personality (mood, behaviors, character, etc.). Besides, data controllers could use very simple, but effective ways to test their users' knowledge of the systems they offer. For example, after the informing activity, 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 it 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 the consent box in, for example, in 5 seconds, this should mean that the user did not read it, so such a case should be avoided. They could also place a button on their websites/services interface, such as the robot's screen or use a verbal indication, about preventing data controllers to trade or share their data with third parties. Such a solution is already available in the California Consumer Privacy Act[538].
- Recently, software developers work on AI-based systems analyzing users' privacy needs and design their systems according to the outcomes reached by these analyses. Companies deploying AI systems could easily use such systems to comply with GDPR. 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[539]. These tools generally help to provide explanations through counterfactuals that would surely help average users to understand the basic concept. There are works ongoing for creating a voice assistant which users can refer questions to understand these counterfactual statements in a natural way and without requiring them to have a technical knowledge to understand the explanations[540]. Additionally, another technique that could generate real-time explanations with the help of computational models (mainly, RL technique) letting the

[538] See, CCPA § 1798.135 (1)

[539] Li, et. al., 2018. Their work focuses on image based processing basically, and we are aware of the fact that systems based on natural language processing might be harder than static visuals like images. However, we do not intend to point one specific solution as a good solution; combination of several solution could help a better legal and ethical compliation. The authors point out that their solution is not a full solution to the problems with transparency of black boxes, but still, is another contribution towards a full solution.

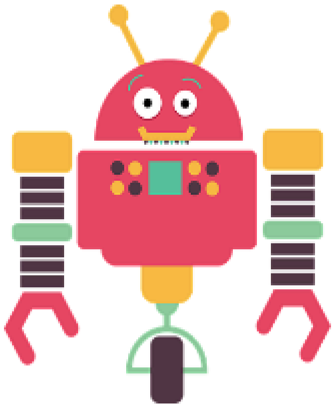
[540] See, Sokol and Flach, 2018.

data subjects to personalize the explanations could be also useful[541]. In our case, we could imagine such a solution. 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”. In this way, excluding Julia’s son from the algorithmic assessment would be quite easy; just a notification to the Company away. This requires data controllers to always and in any case be well aware which variables affected a particular outcome.

- The companies also could use practical tools for detecting their products’ or services’ GDPR compliance in terms of the information or privacy statement and consent requirements. Such tools are already available in the market, but also projects are running in the EU targeting to reach this purpose[542].

2.2. For Users/Data Subjects

- They must be aware of the dark side of the technologies they use.
- They should always be aware that a robot is a machine, although it could humanly interact with them.
- They could place a sign in the entrance and inside of their homes indicating the operation of an HSR. If someone does not wish to be under the surveillance of the robot,



Attention!

Robot under operation

Figure 12. Example warning sign to be placed in the entrance and inside the home.

[541] In their work, Ehsan et al. (2019) developed an automated rationale generation for providing such explanations based on real human explanations used for training a model.

[542] See, http://claudette.eui.eu/about/index.html Last accessed: 15 June 2020.

the user must shut it down and should not create stress on family members and visitors to accept the robot. 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 (will be mentioned below) for the data controllers.

2.3. For Lawmakers

- Bearing in mind the technology's development speed, using scenarios could help make future-friendly legislation to avoid unwanted legal issues.
- They should find a way to embed the standards[543] and make the codes of conduct compulsory for robotic companies to ensure their compliance with the data protection rules.

2.4. For Data Protection Authorities

The first suggestion will be related to enhancing an already existed solution. According to Article 42 of the GDPR, data controllers are called for voluntarily having certificates proving their GDPR compliance approved by the MS, the supervisory authorities, the EDPB, and the Commission. The certification includes not only paperwork but also obtaining seals and marks for their products and services. It would be a clever choice if the new legislation (as the EC's White Paper on Artificial Intelligence suggested) introduce a compulsory certification system for the companies offering services through personal house robots, unlikely the voluntary expression of the GDPR. The certification could be established under at least three criteria:

- Compulsory user education and training under the oversight of the NSA in collaboration with the specific national authorities to the service offered (e.g., National Alzheimer Association). Improving the EU citizens' basic digital skills specific to the MS by 2025 is already an idea raised by the EU Institutions[544].
- 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. This idea is not something new; already, persons who do not have a driving license cannot drive a car legally, and to get the driving license the persons should go

[543] For example, the IEEE project *P7006 - Standard for Personal Data Artificial Intelligence (AI) Agent*, Accessed from: https://standards.ieee.org/project/7006.html. Last accessed: 31 January 2020.

[544] Council of the European Union, 2020, para.57-60.

through driving courses. In this case, no one should be allowed to have a personal robot at home unless having a robot user license. For the robot user licenses case, it should be valid maximum for a year and the user must meet certain criteria to get a new license (e.g. accomplishment of a new training). Such a solution already exists for developers choosing a safeguard plan for themselves against the possible misuse of AI solutions by any user[545]. For a company license, it should be first obtained from the competent authority (e.g. EU Agency for Robotics and Artificial Intelligence[546]) or anew authority set up by the new legislation. Data controllers obtained the certificate could place a seal on their products or services indicating the eligibility of their data processing in line with data protection rules. As one of the opponents to this dissertation suggested, the robot users should register their robots in a central database issued by the related agency which provides the certificates for the data controllers. Unless they register the robotic product and set the data processing credentials themselves, data processing activity should not take place. This means, that there is a need for a central database developed in consultation with the related stakeholders and created in line with the data protection by design and by default rules.

- Compulsory insurance system applicable both for the creators and users of the robot: 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 suffered parties.

Besides the certification:

- The DPAs should raise their knowledge on AI technologies in a technical meaning.
- They should generate more guidelines on AI technologies and should not wait for the EU authorities to deliver some, even though some initial works indicating common implementation have been introduced by the EU institutions during June 2020.
- They could launch pieces of specific training for data controllers on how to design consent and privacy statements.
- Specific explanations on the responsibilities and possible liabilities of the natural persons using AI technologies could be useful.

[545] Responsible AI. Accessed from: https://www.licenses.ai Last accessed: 31 January 2020.
[546] The idea behind this expression could be found in the EP, 2017.

- They could oversee the validity and understandability of the information and consent statements the data controllers provide[547].

Other possible solutions:

- DPIA could be supported with other specific and novel assessment techniques related to the processing of data in AI systems and could be made a prerequisite to earning the certificates. For example, the ethical Technology Assessment accompanied by a data hygiene certificate[548] or Stakeholder Impact Assessment[549] focusing on the social impact and ethical aspects of a certain technology such as AI could offer a possibility to assess even more concrete cases for HSR. The data hygiene certificate proving the logs of the AI development particularly to see the history of the training data (how the data was received, does it raise any bias risk, is it accurate, etc.) could be combined with these assessments and presented to the related authority issuing the certificate.
- In their comprehensive analysis on selected legal scholars discussing ML and its risks, Lehr and Ohm[550] concluded that the legal scholars, sometimes wrongly, miss the assessment of the risks arising from using AI system resulting in a legal effect, because they are lack of technical training that is necessary for them to understand the technology (and one should note that they are referring to the case of supervised learning, only). In this case, the lawyers and legal academia must understand the real and even technical issues behind AI and especially, ML. Promoting AI courses understandable by the legal academia and promoting “AI and law courses” for the lawyers and the developers or robotic companies together with the related national or international authorities could be a practical solution. These courses should be starting from the BA level, if not possible to settle at high schools. There could be pieces of training prepared or offered by the NSAs or Bar Associations[551].
- Suggested revisions on the guidelines or about publishing new guidelines: Several guidelines have been published about the implementation of the GDPR at the EU

[547] Actually, Recital 66 of the Directive 2009/136/EC points granting more powers to enable national authorities such as the NSAs to make informing activities more effective.

[548] A novel solution offered by van Wynsbergh, 2020, p.18.

[549] A novel solution offered by Leslie, 2019, pp. 28-30.

[550] Lehr and Ohm, 2017.

[551] Hungarian Lawyers Association organized a special event entitled Artificial Intelligence and Law on the 28th of November 2019 for the lawyers. A day-long and free of charge event was organized in a way that after each presentation delivered by a professional, participants took an online exam to reinforce their knowledge. The participants collected a certain amount of credits to earn a certificate.

level. If the EU's aim with the GDPR is to ensure a uniform application of the GDPR regardless of whatever field is, then it would make a great impact to provide guidelines specific to AI. Already, the HLEGAI published the so-called ethics guidelines for AI[552], however, data protection specific guidelines prepared by the EDPB would ensure better enforcement in this field. For example, in one of its guidelines, the EDPB gives a great example[553] on how data controllers could ensure the validity of consent they obtained, specific to the informing obligation. The example refers to an imaginary company that receives complaints about the clarity of their purpose indication. The company then goes for a kind of a lab experiment (experimenting with a sample group and surveys) to find out its users' specific information needs and updates its consent information based on that. This example proves that the EDPB could make such specific guidance on a very specific topic like consent and it could be also done for the application of the GDPR on AI technologies. More examples in this sense are already available. ICO, in cooperation with the Alan Turing Institute, already published a guideline on explaining the decisions made with AI[554] is a unique work, in this case. It is worth noting that the Alan Turing Institute also has published another but this time a generic ethics guideline for AI[555].

- If there will be new legislation focusing on the regulation of AI technologies which is highly-likely based on the current policy papers generated by the EU institutions, standards should not be left out of the picture. ISO's standards for robotics or standards very specific to a particular technology, like the one published by the Society of Automotive engineering for automated driving systems[556], or the IEEE's initiative on creating a standard for ethical aspects of AI[557] including a specific sub-principle on privacy could guide the EU law-maker in this sense.
- "AI should be understood as a socio-technical system and should be assessed according to the society in which it has been created, further, society's role in the development and applications of AI/ML should not be underestimated"[558]. It should be beard in mind that not all AI applications have the same weight in terms of a legal

[552] HLEGAI, 2019b.
[553] EDPB, 2020b, para. 73, Example 12.
[554] ICO, 2020.
[555] Leslies, 2019.
[556] See, SAE J3016 and J3018, Available here: https://www.sae.org/standards/content/j3018_201909/?src=j3016_201806 Last accessed: 25 July 2020.
[557] IEEE, BSI8611 on "Robots and Robotic Devices: Guide to the Ethical Design and Application of Robots and Robotic Systems."
[558] van Wynsbergh, 2020, p.15.

effect in a person’s life, even though the risk level might be considered high. Public debate on each type of AI application or a group of similar applications that are planned to be developed could be launched via surveys. This could be either done at the MS level (if the developer is a public institution) or at the EU level (if the product or the service is offered by a public institution or private company of a non-EU country).

Finally, we believe that more interdisciplinary studies, like we did here, should be encouraged in academia to translate each other’s language in a mutually understandable way. Those studies could be also conducted by the government in the frame of public education and awareness-raising programs. On the other hand, inter-legal studies could also help law-makers not to invent the tire again, but benefit from the existed legal rules in another fields of law. For example, even though there are different legislation and authorities ensuring consumer protection, it often intersects with data protection especially in terms of AI applications and the use of algorithmic decision-making tools. Legal scholars and researchers in the consumer protection field often argue price discrimination, invalid consent practices, and other issues arising from AI applications. Big Data triggers anticipation or modification of consumer behaviors[559] illegally and the data processed in this way, in the end, is personal data. Consumers, in the end, are data subjects. However, the researches in the consumer protection field seem more profound than the ones in data protection. Consumer protection scholars research consumer behaviors to understand the reasons for their choices including their consent choices. Interaction between these two fields, without a doubt, could enhance the inputs for identifying a variety of solutions in the data protection field.

[559] Sartor, 2020a, p.18.

Bibliography

Articles

Adadi, A., Berrada, M. (2018). "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)," IEEE Access, 6, pp. 52138-52160, doi: 10.1109/ACCESS.2018.2870052

Ahonen P. et al. (2008) Dark scenarios. In: Wright D., Friedewald M., Punie Y., Gutwirth S., Vildjiounaite E. (eds) Safeguards in a World of Ambient Intelligence. The International Library of Ethics, Law and Technology, vol 1. Springer, Dordrecht, pp.33-142

Alves de Lima Sarge, C.and Berente, N. (2017) Computing Ethics. Is That Social Bot Behaving Unethically? A procedure for reflection and discourse on the behavior of bots in the context of law, deception, and societal norms. Communications of the ACM, 60(9): 29-31.

Ananny, M., Crawford, K. (2018) 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability', New Media & Society, 20(3), pp. 973–989. doi: 10.1177/1461444816676645.

Armstrong, J. S. and Green, K. C. (2018) 'Forecasting Methods and Principles: Evidence-Based Checklists. Journal of Global Scholars of Marketing Science'. Available at SSRN: https://ssrn.com/abstract=3218788

Arulkumaran, K, Deisenroth M.P., Brundage, and M. Bharath ,A.A. (2017) 'A brief survey of deep reinforcement learning' arXiv preprint: arXiv:1708.05866.

Augusto, J. C., Kramer, D., Alegre, U., Covaci, A. and Santokhee, A. (2018) The user-centred intelligent environments development process as a guide to co-create smart technology for people with special needs. Universal Access in the Information Society, 17 (1). pp. 115-130. ISSN 1615-5289 (doi:10.1007/s10209-016-0514-8)

Ballard, S. and Calo, R. (2019) 'Taking Futures Seriously: Forecasting as Method in Robotics Law and Policy', We Robot 2019, University of Miami, School of Law.

Balogh, Z. G., Polyák, G., Rátai, B., Szőke, G. L. (2012) 'Privacy in the Workplace', Studia Iuridica Auctoritate Universitatis Pecs Publicata, 150, pp. 9–40.

Barfield W. (2018) ‘Liability for Autonomous and Artificially Intelligent Robots’, Paladyn, Journal of Behavioral Robotics, p. 193-203. doi: 10.1515/pjbr-2018-0018.

Baumer, E. P. S. et al. (2018) ‘What Would You Do? Design Fiction and Ethics’, in Proceedings of the 2018 ACM Conference on Supporting Groupwork. New York, NY, USA: ACM (GROUP ’18), pp. 244–256. doi: 10.1145/3148330.3149405

Bisconti Lucidi, P. and Nardi, D. (2018) ‘Companion Robots: The Hallucinatory Danger of Human-Robot Interactions’, in Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society. New York, NY, USA: ACM (AIES ’18), pp. 17–22. doi: 10.1145/3278721.3278741.

Bleecker, J. (2009) Design Fiction: A short essay on design, science, fact and fiction. Near Future Laboratory.

Blythe, M. (2014) ‘Research Through Design Fiction: Narrative in Real and Imaginary Abstracts’, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems New York, NY, USA: ACM (CHI ’14), pp. 703–712. doi: 10.1145/2556288.2557098.

_ (2017) ‘Research Fiction: Storytelling, Plot and Design’, in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: ACM (CHI ’17), pp. 5400–5411. doi: 10.1145/3025453.3026023.

Broman, M. M. and Finckenberg-Broman, P. (2017) ‘Human-Robotics&AI interaction: The Robotics/AI legal entity (RAiLE©)’, in 2017 IEEE International Symposium on Technology and Society (ISTAS), pp. 1–7. doi: 10.1109/ISTAS.2017.8318980.

Bruno, B., Young Chong, N., Kamide, H., Kanoria, S., Lee, J., Lim, Y., Pandey, A. K., Papadopoulos, C., Papadopoulos, I., Pecora, F., Saffiotti, A., Sgorbissa, A. (2017) ‘The {CARESSES} EU-Japan project: making assistive robots culturally competent’, CoRR, abs/1708.06276. Available at: http://arxiv.org/abs/1708.06276.

Burrell, J. (2016) ‘How the machine “thinks”: Understanding opacity in machine learning algorithms’, Big Data & Society, 3(1), pp. 1-12. doi: 10.1177/2053951715622512.

Butler, O. (2015) ‘The Expanding Scope of the Data Protection Directive: The Exception for a 'Purely Personal or Household Activity’, Cambridge Legal Studies Research Paper Series, 54/2015, Available at: https://ssrn.com/abstract=2660916

Calo, R. (2015) 'Robotics and the Lessons of Cyberlaw', California Law Review, 103, pp. 513–532.

Carlini, N., Chang L., Jernej K., Úlfar E. and Dawn, X.S. (2018) "The Secret Sharer: Measuring Unintended Neural Network Memorization & Extracting Secrets." CoRR. Available at: abs/1802.08232

Carmichael, L., Stalla-Bourdillon, S. and Staab, S. (2016) 'Data Mining and Automated Discrimination: A Mixed Legal/Technical Perspective', IEEE Intelligent Systems, 31(6), pp. 51–55. doi: 10.1109/MIS.2016.96.

Carlsen, H. Johansson, L., Wikman-Svahn, P., Dreborg, K. H. (2014) 'Co-evolutionary scenarios for creative prototyping of future robot systems for civil protection', Technological Forecasting and Social Change, 84, pp. 93–100. doi: https://doi.org/10.1016/j.techfore.2013.07.016

Casey, B.J., Farhangi, A., & Vogl, R. (2019). "Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise". Berkeley Technology Law Journal, 34:145, https://ssrn.com/abstract=3143325

Cath, C. (2018). "Governing artificial intelligence: ethical, legal and technical opportunities and challenges", Phil. Trans. R. Soc. A.376. https://doi.org/10.1098/rsta.2018.0080.

Conti, M. and Passarella, A. (2018) 'The Internet of People: A human and data-centric paradigm for the Next Generation Internet', Computer Communications, 131, pp. 51–65. doi: https://doi.org/10.1016/j.comcom.2018.07.034.

Coopamootoo, K.P.L. and Groß, T. (2017) 'Why Privacy Is All but Forgotten an Empirical Study of Privacy & Sharing Attitude', Proceedings on Privacy Enhancing Technologies, (4):39–60

Coulton, P, Lindley, J and Akmal, H.A. (2016) Design fiction: does the search for plausibility lead to deception? in P Lloyd & E Bohemia (eds), Proceedings of Design Research Society Conference 2016. Proceedings of DRS 2016, vol. 1, Design Research Society, pp. 369-384, DRS 2016: Future Focused Thinking, Brighton, United Kingdom, 27/06/16. https://doi.org/10.21606/drs.2016.148

Custers, B., Dechesne, F., Sears, A.M., Tani, T., van der Hof, S. (2018) A comparison of data protection legislation and policies across the EU, Computer Law & Security Review 34, 234–243.

Custers, B.H.M., Hof, S. van der, Schermer, B.W., Appleby-Arnold, S. Brockdorff, N (2013). '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, 10, pp.435–457.

Darling, K. (2017). Who's Johnny? Anthropomorphic framing in human-robot interaction, integration, and policy (preliminary draft), We Robot 2015

de Andrade, N. N. G. (2012) 'The application of future-oriented technology analysis (FTA) to law: the cases of legal research, legislative drafting and law enforcement', Foresight, Vol. 14 Issue: 4, pp.336-351, https://doi.org/10.1108/14636681211256116

de Graaf, M. M. A. (2016) 'An Ethical Evaluation of Human–Robot Relationships', International Journal of Social Robotics, 8(4), pp. 589–598. doi: 10.1007/s12369-016-0368-5.

de Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., González Fuster, G. (2009) 'Legal safeguards for privacy and data protection in ambient intelligence', Personal and Ubiquitous Computing, 13(6), pp. 435–444. doi: 10.1007/s00779-008-0211-6.

Denning, T., Matuszek, C., Koscher, K., Smith, J. R., Kohno, T. (2009) 'A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons', in Proceedings of the 11th International Conference on Ubiquitous Computing. New York, NY, USA: ACM (UbiComp '09), pp. 105–114. doi: 10.1145/1620545.1620564.

Dourish, P. and Bell, G. (2014) 'Resistance is futile'': reading science fiction alongside ubiquitous computing', Personal and Ubiquitous Computing, 18(4), pp. 769–778. doi: 10.1007/s00779-013-0678-7.

Duffy, B. R., Rooney, C. F. B., O'Hare, G. M. P., and O'Donoghue, R. P. S. (1999) What is a Social Robot? in 10th Irish Conference on Artificial Intelligence & Cognitive Sciences, September 1-3 1999.

Edwards, C., Edwards, A., Spence, P. R., Xialing, L. (2018) 'I, teacher: using artificial intelligence (AI) and social robots in communication and instruction', Communication Education. Routledge, 67(4), pp. 473–480. doi: 10.1080/03634523.2018.1502459.

Ehsan, U., Tambwekar, P., Chan, L., Harrison, B., Riedl, M. (2019). “Automated Rationale Generation: A Technique for Explainable AI and its Effects on Human Perceptions”, arXiv, Available at: arXiv:1901.03729.

Everson, E. (2016) “Privacy by Design: Taking Ctrl of Big Data,”, Cleveland State Law Review, vol. 65. pp. 27–44,

Felzmann, H., Fosch-Villaronga, E., Lutz, C. and A. Tamo-Larrieux (2019), Robots and Transparency the Multiple Dimensions of Transparency in the Context of Robot Technologies, eLawWorking Paper Series, 29 April 2019.

Finale, D.V., Kortz, M. (2017). “Accountability of AI Under the Law: The Role of Explanation”, Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working paper. Available at: https://dash.harvard.edu/handle/1/34372584

Floridi, L., and Sanders, J. W. (2004). On the morality of artificial agents. Minds and machines, 14(3), 349-379.

Fong, T., Nourbakhsh, I., Dautenhahn, K. (2003) “A survey of socially interactive robots” Robotics and Autonomous Systems 42, pp. 143–166.

Fosch-Villaronga E. and Albo-Canals J. (2019) ‘“I’ll take care of you,” said the robot’, Paladyn, Journal of Behavioral Robotics, p. 77. doi: 10.1515/pjbr-2019-0006.

Fosch Villaronga, E, Felzmann, H, Pierce, R, de Conca, S, de Groot, A, Robins, S & Ponce Del Castillo, a (2018) “Nothing comes between my robot and me: Privacy and human-robot interaction in robotised healthcare”. in R Leenes, R van Brakel, S Gutwirth & P de Hert (eds), Data protection and privacy: The internet of bodies. 1 edn, Computers, Privacy and Data Protection, Hart Publishing, pp. 135-170.

Frank, L. and Nyholm, S. (2017) ‘Robot sex and consent: Is consent to sex between a robot and a human conceivable, possible, and desirable?’, Artificial Intelligence and Law, 25(3), pp. 305–323. doi: 10.1007/s10506-017-9212-y.

Gellert, R. and Gutwirth, S. (2013) ‘The legal construction of privacy and data protection’, Computer Law & Security Review, 29(5), pp. 522–530. doi: https://doi.org/10.1016/j.clsr.2013.07.005.

Giles, C. (2015) “Balancing the breach: Data privacy laws in the wake of the NSA revelations”, Houston Journal of International Law 37, 2.

Gonzatto, R. F. et al. (2013) ‘The ideology of the future in design fictions’, Digital Creativity. Routledge, 24(1), pp. 36–45. doi: 10.1080/14626268.2013.772524.

Goodman, B. and Flaxman, S. (2017) “European Union Regulations on Algorithmic Decision-Making and a ‘Right to Explanation’”, AI Magazine, 38(3), pp. 50-57. doi: 10.1609/aimag. v38i3.2741.

Grimmelmann, J. and Westreich, D. (2017) ’Incomprehensible Discrimination’, Calif L Rev Online, 7, pp. 164–177

Gültekin Várkonyi, G. 2017a “Evaluation on Turkey's Data Protection Adventure”, EDPL, 3, 238.

_ 2017b “Tasarımda Veri Koruma: Kişisel Veri Dostu Yazılımlar İçin Hukuki, İdari ve Teknik Bir Yaklaşım”, Proceedings of the 10th International Conference on Information Security and Cryptology: Cyber Security and Artificial Intelligence, 20-21 October 2017, Ankara, Turkey.

_2017c “Yolcu İsim Kayıtlarının Terörle Mücadele Kapsamında Yurt Dışına Yasal Aktarımı: Avrupa Birliği Uygulamaları ve Türkiye”, TBB, 132, 340-382.

_2019 “Operability of the GDPR’s Consent Rule in Intelligent Systems: Evaluating the Transparency Rule and the Right to Be Forgotten”, in Intelligent Environments, Andrés Muñoz, Sofia Ouhbi, Wolfgang Minker, Loubna Echabbi, Miguel Navarro-Cía (eds.), IOS Press.

Haarnoja,T., Zhou,A., Hartikainen, K., Tucker, G., Ha, S., Tan, J., Kumar, V., Zhu, H., Gupta, A., Abbeel, P., Levine, S.(2019). Soft Actor-Critic Algorithms and Applications. Pre-print version in https://arxiv.org/abs/1812.05905

Hallevy, G., (2010) The Criminal Liabiliıty of Artificial Intelligence Entities-From Science Fiction to Legal Social Control. Akron Intellectual Property Journal, 4(2).

Hegel, F., Muhl, C., Wrede, B. Hielscher-Fastabend, M., and Sagerer, G. (2009) ‘Understanding Social Robots’, in Proceedings of the 2009 Second International

Conferences on Advances in Computer-Human Interactions. Washington, DC, USA: IEEE Computer Society (ACHI ’09), pp. 169–174. doi: 10.1109/ACHI.2009.51.

Hoofnagle, C. J., van der Sloot, B. and Borgesius, F. Z. (2019) ‘The European Union general data protection regulation: what it is and what it means’, Information & Communications Technology Law. Routledge, 28(1), pp. 65–98. doi: 10.1080/13600834.2019.1573501.

Ishii, K. (2019) ‘Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects.’, AI Soc., 34(3), pp. 509–533. doi: 10.1007/s00146-017-0758-8.

Kamarinou, D., Millard, C., Singh, J., (2016) Machine Learning with Personal Data. Technical Report. Queen Mary School of Law Legal Studies Research Paper, 19, 2, pp.194-208.

Karnow, E.A. C. (1994) The Encrypted Self: Fleshing Out the Rights of Electronic Personalities, J. Marshall J.Computer & Info. L. 13, 1, pp. 1-16.

Karyda, M, Gritzalis, S., Park, H.J., Kokolakis, S. (2009) "Privacy and fair information practices in ubiquitous environments: Research challenges and future directions”. Internet Research, 19(2)

Katyal S.K. (2019) “Private Accountability in the Age of Artificial Intelligence”, UCLA L. Rev. 54. pp. 66-141.

Kemper, J., Kolkman, D. (2019) Transparent to whom? No algorithmic accountability without a critical audience, Information, Communication & Society, 22:14, 2081-2096, DOI: 10.1080/1369118X.2018.1477967.

Kerr, I.R., Bornfreund, M., (2005) Buddy Bots: How Turing’s Fast Friends Are Undermining Consumer Privacy. Presence: Teleoperators and Virtual Environments, 14, 6.

Kim, T. and Hinds, P. (2006) ‘Who Should I Blame? Effects of Autonomy and Transparency on Attributions in Human-Robot Interaction’, in ROMAN 2006 - The 15th IEEE International Symposium on Robot and Human Interactive Communication, pp. 80–85. doi: 10.1109/ROMAN.2006.314398.

Kirchberger, T. (2017) ’European Union Policy-Making on Robotics and Artificial Intelligence: Selected Issues’, Volume 13, Croatian Yearbook of European Law and Policy, p. p197

Kokott, J. and Sobotta, C., (2013), The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, 2013, Vol. 3, No. 4

Koops, BJ, Newell, B, Timan, T, Skorvánek, I, Chokrevski, T & Galič, M., (2017) 'A typology of privacy', University of Pennsylvania Journal of International Law, vol. 38, no. 2, pp. 483-575.

Korn, O., Bieber, G. and Fron, C. (2018) ‘Perspectives on Social Robots: From the Historic Background to an Experts’ View on Future Developments’, in Proceedings of the 11th PErvasive Technologies Related to Assistive Environments Conference. New York, NY, USA: ACM (PETRA’18), pp. 186–193. doi: 10.1145/3197768.3197774.

Kosinski, M., Stillwell, D. and Graepel, T., (2013) ‘Private traits and attributes are predictable from digital records of human behavior’, Proceedings of the National Academy of Sciences, 110(15), pp. 5802 LP – 5805. doi: 10.1073/pnas.1218772110.

Körtner, T. (2016). ‘Ethical challenges in the use of social service robots for elderly people’ Zeitschrift für Gerontologie und Geriatrie, 4, pp. 303-307. DOI 10.1007/s00391-016-1066-5

Lake, B. M., Ullman, T. D., Tenenbaum, J. B. and Gershman, S. J. (2017) “Building machines that learn and think like people,” Behavioral and Brain Sciences. Cambridge University Press, 40, p. e253. doi: 10.1017/S0140525X16001837

LaRosa, E. and Danks, D. (2018) ‘Impacts on Trust of Healthcare AI’, in Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society. New York, NY, USA: ACM (AIES ’18), pp. 210–215. doi: 10.1145/3278721.3278771.

Laukyte, M. (2013). ‘The capabilities approach as a bridge between animals and robots’, EUI MWP, 2013/05, Cadmus, European University Institute Research Available at: http://hdl.handle.net/1814/27058

Lehr, D., Ohm, P. (2017). “Playing with the Data: What Legal Scholars Should Learn About Machine Learning”, UCDL Review 51, pp. 653- 671.

Le Métayer, D., Monteleone, S. (2009) “Automated consent through privacy agents: legal requirements and technical architecture”. Computer Law and Security Review, Elsevier, 25 (2), pp.136-144.

Leyzberg, D., Ramachandran, A., and Scassellati, B. (2018) ‘The Effect of Personalization in Longer-Term Robot Tutoring’, ACM Transactions on Human-Robot Interaction, Vol. 7, No. 3, Article no. 19.

Li, O., Liu, H., Chen, C., Rudin, C. (2018). eep Learning for Case-Based Reasoning through Prototypes: A Neural Network that Explains Its Predictions. Available at arXiv: https://arxiv.org/abs/1710.04806.

Li, T., Villaronga, E. F., Kieseberg, P. (2017). Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018186

Li, X., Jiang, H., (2017). Artificial Intelligence Technology and Engineering Applications. Applied Computational Electromagnetics Society Journal, 32(5), pp. 381-388.

Lindley, J., Akmal, H. & Coulton, P. (2020). Design Research and Object-Oriented Ontology. Open Philosophy, 3(1), pp. 11-41. Retrieved 31 Jan. 2020, from doi:10.1515/opphil-2020-0002

Lynskey, O., (2011) ‘Track[ing] changes: an examination of EU Regulation of online behavioural advertising through a data protection lens’, European Law Review, Sweet & Maxwell, pp. 874-886.

Manikonda, L., Deotale, A. and Kambhampati, S. (2017) ‘What’s up with Privacy? User Preferences and Privacy Concerns in Intelligent Personal Assistants.’, CoRR. Available at: http://arxiv.org/abs/1711.07543.

Matthias, A. (2004) ‘The responsibility gap: Ascribing responsibility for the actions of learning automata’, Ethics and Information Technology, 6(3), pp. 175–183. doi: 10.1007/s10676-004-3422-1.

Mejía, C. and Kajikawa, Y. (2019) ‘Technology news and their linkage to production of knowledge in robotics research’, Technological Forecasting and Social Change, 143, pp. 114–124. doi: https://doi.org/10.1016/j.techfore.2019.03.016.

Mikolov, T., Joulin, A., Baroni, M. (2018) “A Roadmap Towards Machine Intelligence.” Lecture Notes in Computer Science, pp. 29–61.

Miller, J., Williams, A. B. and Perouli, D. (2018) ‘A Case Study on the Cybersecurity of Social Robots’, in Companion of the 2018 ACM/IEEE International Conference on Human-Robot Interaction. New York, NY, USA: ACM (HRI ’18), pp. 195–196. doi: 10.1145/3173386.3177078.

Millar, J., and Kerr, I. (2016). Delegation, relinquishment, and responsibility: The prospect of expert robots. In Robot Law, Cheltenham, UK: Edward Elgar Publishing. https://doi.org/10.4337/9781783476732.00012.

Minkkinen, M. (2015) ‘Futures of privacy protection: A framework for creating scenarios of institutional change’, Futures, 73, pp. 48–60. doi: https://doi.org/10.1016/j.futures.2015.07.006.

Misek, J., (2014) ‘Consent to Personal Data Processing - The Panacea or the Dead End’, Masaryk University Journal of Law and Technology, 8.1, pp. 69–83.

Mittelstadt B.D., Allo P., Taddeo M., Wachter S. and Floridi L. (2016) The ethics of algorithms: Mapping the debate, Big Data & Society, 3(2), pp. 1-21

Moerman, C. J., van der Heide, L. and Heerink, M. (2019) ‘Social robots to support children’s well-being under medical treatment: A systematic state-of-the-art review’, Journal of Child Health Care, 23(4), pp. 596–612. doi: 10.1177/1367493518803031.

Monroe, D. (2018) ‘AI, Explain Yourself’, Commun. ACM. New York, NY, USA: Association for Computing Machinery, 61(11), pp. 11–13. doi: 10.1145/3276742.

Mostert, M., Bredenoord, A. L., van der Sloot, B., van Delden, J. J. M. (2017). ’From Privacy to Data Protection in the eu: Implications for Big Data Health Research’, European Journal of Health Law. Leiden, The Netherlands: Brill | Nijhoff, 25(1), pp. 43–55. doi: https://doi.org/10.1163/15718093-12460346.

Mulligan, C. (2018) ‘Revenge against Robots’, 69 S. C. L. Rev. 579.

Müller, V. C. and Bostrom, N. (2016) ‘Future progress in artificial intelligence: A survey of expert opinion’, in Vincent C. Müller (ed.), Fundamental Issues of Artificial Intelligence, Synthese Library; Berlin: Springer, pp. 553-571

Nath, R. and Sahu, V. (2017) ‘The problem of machine ethics in artificial intelligence’, AI & SOCIETY. doi: 10.1007/s00146-017-0768-6.

Nussbaum, M. C. (2004). Beyond “Compassion and Humanity:” Justice for Non-Human Animals. In Animal Rights. Current Debates and New Directions. Eds. C. R. Sunstein, and M. C. Nussbaum, 299–320. New York: Oxford University Press.

O'Sullivan, S., Nevejans, N., Allen, C., Blyth, A., Leonard, S., Pagallo, U., Holzinger, K., Holzinger, A., Sajid, M. I., Ashrafian, H. (2019). Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. The international journal of medical robotics + computer assisted surgery: MRCAS, 15(1), e1968. https://doi.org/10.1002/rcs.1968

Ratcliffe, J. (2002). ‘Scenario planning: strategic interviews and conversations’, Foresight, Vol. 4 Issue: 1, pp.19-30, https://doi.org/10.1108/14636680210425228

Rhoen, M. and Feng, Q. Y. (2018) ‘Why the “Computer says no”: illustrating big data’s discrimination risk through complex systems science’, International Data Privacy Law, 8(2), pp. 140–159. doi: 10.1093/idpl/ipy005.

Richards, N., and Smart, W. (2016). How should the law think about robots? In R. Calo, A.M. Froomkin, & I. Kerr (Eds.), Robot Law (3-22). Northampton, MA: Edward Elgar Publishing.

Richert, A., Müller, S., Schröder, S., Jeschke S. (2018) Anthropomorphism in social robotics: empirical results on human–robot interaction in hybrid production workplaces, AI & SOCIETY, 33(3), pp. 413–424. doi: 10.1007/s00146-017-0756-x.

Rossnagel, A., Tamer, B., Friedewald, M., Geminn, C. Grigorjew, O., Karaboga, M., Nebel, M. (2018) National Implementation of the General Data Protection Regulation: Challenges, Approaches, Strategies. Policy Paper, Karlsruhe: Forum Privacy and Self-Determined Life in the Digital World.

Sandra Wachter & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, (2019) Colum. Bus. L. Rev. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

Sandvig, C., Hamilton. K, Karahalios, K., Langbort, C. (2016) ‘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). Available at: http://ijoc.org/index.php/ijoc/article/view/6182/1807

Sántáné-Tóth E. (2007). 'Artificial Intelligence in Hungary – the first 20 years', Proceedings of Workshop of MEDICHI 2007, ed.: Böszörményi L., Klagenfurt, April 12-13 2007, pp. 74-88.

Santoro, M., Marino, D. and Tamburrini, G. (2008) 'Learning robots interacting with humans: from epistemic risk to responsibility', AI & SOCIETY, 22(3), pp. 301–314. doi: 10.1007/s00146-007-0155-9.

Selbst, A. D. and Powles, J. (2017) 'Meaningful information and the right to explanation', International Data Privacy Law, 7(4), pp. 233–242. doi: 10.1093/idpl/ipx022.

Schönberger, D. (2019) "Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications", International Journal of Law and Information Technology, 27, pp. 171–203.

Sokol, K., Flach, P. (2018). "Glass-Box: Explaining AI Decisions With Counterfactual Statements Through Conversation With a Voice-enabled Virtual Assistant"., Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, pp. 5868-5870.

Stahl, C.B., Wright, D. (2018). "Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation," IEEE Security & Privacy, vol. 16, no. 3, pp. 26-33. doi: 10.1109/MSP.2018.2701164.

Suresh, H., Guttag, J. V. (2020). A Framework for Understanding Unintended Consequences of Machine Learning. Available at: https://arxiv.org/pdf/1901.10002v3.pdf.

Syrdal, D.S., Walters, M., Otero, N.R., Koay, K.L., Datenhahn, K. (2007) "He knows when you are sleeping - Privacy and the Personal Robot", Technical Report from the AAAI 2007 Workshop: W06 on Human Implications of Human-Robot Interaction, AAAI Press, pp. 28–33.

Svantesson, D. J. B. (2015) "The (Uncertain) Future of Online Data Privacy", 9 Masaryk U. J.L. & Tech., pp. 129-153.

Štitilis, D. and Laurinaitis, M. (2017) ‘Treatment of biometrically processed personal data: Problem of uniform practice under EU personal data protection law’, Computer Law & Security Review, 33(5), pp. 618–628. doi: https://doi.org/10.1016/j.clsr.2017.03.012

Taddy, M. (2019). The Technological Elements of Artificial Intelligence, in: The Economics of Artificial Intelligence: An Agenda, Ajay Agrawal, Joshua Gans, and Avi Goldfarb (eds.), University of Chicago Press, National Bureau of Economic Research, 61 - 87.

Tan, K.-H. and Lim, B. P. (2018) “The artificial intelligence renaissance: deep learning and the road to Human-Level machine intelligence,” APSIPA Transactions on Signal and Information Processing. Cambridge University Press, 7, p. e6. doi: 10.1017/ATSIP.2018.6.

Tang, J., Korolova, A., Bai, X., Wang, X. & Wang, X. (2017), 'Privacy Loss in Apple's Implementation of Differential Privacy on MacOS 10.12.', CoRR. Accessed from: abs/1709.02753.

Tjoa, E., Guan, C. (2019) ‘A Survey on Explainable Artificial Intelligence (XAI): Towards Medical XAI’, Pre-print version in: arXiv:1907.07374

Trimmel, M. (2017) ‘Homo informaticus: Thinking and moral values of humans are shaped by human-computer-interaction'. Res Rev Insights 1: DOI: 10.15761/RRI.1000106 227, pp. 1-4.

Tucker, C., (2019) Privacy, Algorithms and Artificial Intelligence (preliminary drafts). In A. K., J. Gans, A. Goldfarb, eds. Economics of Artificial Intelligence. University of Chicago Press. pp. 423-437.

Tyagi, A., (2016) Essay: Artificial Intelligence: Boon or Bane? [Online] SSRN Electronic Journal, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2836438

Tzanou, M. (2015) ‘The War against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security Research Article’, Utrecht Journal of International and European Law, 31(80), pp. 87–103. doi: http://:doi.org/10.5334/ujiel.cq.

Tzirakis, P., Trigeorgis, G., Nicolaou, M., Schuller, B. W., Zafeiriou, S. (2017) ‘End-to-End Multimodal Emotion Recognition Using Deep Neural Networks’, IEEE Journal of Selected Topics in Signal Processing, 11(8), pp. 1301–1309. doi: 10.1109/JSTSP.2017.2764438.

van den Hoven van Genderen, R. (2017) ‘Privacy and data protection in the age of pervasive technologies in AI and robotics’, European Data Protection Law 3, 3.

van Otterlo, M. (2018) “Gatekeeping Algorithms with Human Ethical Bias: The Ethics of Algorithms in Archives, Libraries and Society”. https://arxiv.org/abs/1801.01705.dPS

Veale, M. and Edwards, L. (2018) ‘Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling’, Computer Law & Security Review, 34(2), pp. 398–404. doi: https://doi.org/10.1016/j.clsr.2017.12.002.

Veale M, Binns R, Edwards L. (2018) “Algorithms that remember: model inversion attacks and data protection law” Phil. Trans. R. Soc. A 376: 20180083. http://dx.doi.org/10.1098/rsta.2018.0083

Vitale, J., Tonkin, M., Ojha, S., Williams, M., Wang, X., and Judge, W. (2017). Privacy by Design in Machine Learning Data Collection: A User Experience Experimentation, The AAAI 2017 Spring Symposium on Designing the User Experience of Machine Learning Systems Technical Report SS-17-04, pp. 439-42.

Wachter, S., Mittelstadt, B., Russell, C. (2018) ‘Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR’, Harvard Journal of Law & Technology, 31, 2, pp. 842-887.

Wachter, S., Mittelstadt, B. and Floridi, L. (2017) ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’, International Data Privacy Law, 7(2), pp. 76–99. doi: 10.1093/idpl/ipx005.

Weber, K. M., Gudowsky, N. and Aichholzer, G. (2019) ‘Foresight and technology assessment for the Austrian parliament — Finding new ways of debating the future of industry 4.0’, Futures, 109, pp. 240–251. doi: https://doi.org/10.1016/j.futures.2018.06.018.

Whitley, E. A., and Pujadas, R. (2018). Report on a study of how consumers currently consent to share their financial data with a third party, Financial Services Consumer Panel.

Wisman, T. H. A. (2013) 'Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things' European Journal of Law and Technology, vol. 2013, no. 2, 3.

Wong, R. Y., Merrill, N. and Chuang, J. (2018) 'When BCIs Have APIs: Design Fictions of Everyday Brain-Computer Interface Adoption', in Proceedings of the 2018 Designing Interactive Systems Conference. New York, NY, USA: ACM (DIS '18), pp. 1359–1371. doi: 10.1145/3196709.3196746.

Wright, D. and Raab, C. (2014) 'Privacy principles, risks and harms.', International Review of Law, Computers & Technology. Routledge, 28(3), pp. 277–298. Available at: http://10.0.4.56/13600869.2014.913874.

Wright, D., Finn, R., Gellert, R., Gutwirth, S., Schütz, P., Friedewald, M., Venier, S., Mordini, E. (2014) "Ethical dilemma scenarios and emerging technologies",Technological Forecasting and Social Change, 87, pp.325-336, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2013.12.008.

Youyou, W., Kosinski, M., Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. Proceedings of the National Academy of Sciences, USA, 112, 1036–1040.

Yu, R. and Alì, G. S. (2019) "What's Inside the Black Box? AI Challenges for Lawyers and Researchers," Legal Information Management. Cambridge University Press, 19(1), pp. 2–13. doi: 10.1017/S1472669619000021.

Zimmeck, S, Wang, Z, Zou, L, Iyengar, R, Liu, B, Schaub, F, Wilson, S, Sadeh, N, Bellovin, SM & Reidenberg, J (2017) 'Automated Analysis of Privacy Requirements for Mobile Apps'. in Proceedings 2017 Network and Distributed System Security Symposium. Proceedings 2017 Network and Distributed System Security Symposium, Korea Society of Internet Information, Reston, VA. https://doi.org/10.14722/ndss.2017.23034

Zimmermann, G., Ableitner, T. and Strobbe, C. (2017) 'User Needs and Wishes in Smart Homes: What Can Artificial Intelligence Contribute?', in 2017 14th International Symposium on Pervasive Systems, Algorithms and Networks & 2017 11th International Conference on Frontier of Computer Science and Technology & 2017 Third International Symposium of Creative Computing (ISPAN-FCST-ISCC), pp. 449–453. doi: 10.1109/ISPAN-FCST-ISCC.2017.66.

Books

Alpaydın, E. Machine Learning: The New AI. The MIT Press, 2016. ISBN: 9780262529518

Bostrom, N., (2014) Superintelligence: paths, dangers, strategies First edition, Oxford: Oxford University Press,

Breazeal, C. (2002) Designing Sociable Robots. Cambridge, MA, USA: MIT Press.

Glenn, J. C., Theodore, J. G. (2009) 'Futures Research Methodology Version 3.0', The Millennium Project; 3.0 edition.

Gutwirth, S. and Hildebrant, M (2010). Some Caveats on Profiling / Serge Gutwirth, Yves Poullet, Paul De Hert, (editors). Dordrecht; New York: Springer, c2010.

Jentzsch, N. (2007) Financial privacy: an international comparison of credit reporting systems, 2nd ed., Berlin: Springer.

Lomio, J. P., Wilson, G. W, Spang-Hanssen, H., Djof (2011). Legal Research Methods in a Modern World: A Coursebook. Publishing, 2011, ISBN: 9788757424676.

Microsoft Corporation, (2018). The Future Computed: Artificial Intelligence and its Role in Society. Retrieved from: https://news.microsoft.com/cloudforgood/_media/downloads/the-future-computed-english.pdf

Murphy, R.R. (2001). Introduction to AI Robotics. MIT Press, 2001.

Nussbaum, M. C. (2011). Creating Capabilities. The Human Development Approach. Cambridge, London: The Belknap Press of Harvard University Press.

Packin, N., and Lev-Aretz, Y. (2018). Learning algorithms and discrimination. In Research Handbook on the Law of Artificial Intelligence, Cheltenham, UK: Edward Elgar Publishing.

Technológia jog – Robotjog – Cyberjog (2018), Klein, T., Tóth, A. (eds.), Wolters Kluwer, ISBN: 978 963 295 750.

Voigt, P., von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing, eBook ISBN: 978-3-319-57959-7.

Watkins, D., & Burton, M. (2013). Research methods in law. London, Routledge.

Legislation and Court Cases

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector OJ L 201, 31.7.2002, p. 37–47

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) (Text with EEA relevance)

Case 43-71 Politi s.a.s. v Ministry for Finance of the Italian Republic, [1971], Judgment of the Court, Case no 61971J0043.

Case 39-72, Commission of the European Communities v Italian Republic. Premiums for slaughtering cows [1973] Judgment of the Court, ECLI:EU:C:1973:13.

Case C-101/01, Bodil Lindqvist. [2003], Judgement of the Court, ECLI:EU:C:2003:596.

Case C486/12, X [2013], Judgement of the Court, ECLI:EU:C:2013:836.

C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, [2014], Judgement of the Court, ECLI:EU:C:2014:2428.

Case C-362/14 Maximillian Schrems v Data Protection Commissioner, [2015] Judgement of the Court, ECLI:EU:C:2015:650.

Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, [2016], Judgment of the Court, ECLI:EU:C:2016:779.

Case C-203/15 Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, [2016] Judgement of the Court, ECLI:EU:C:2016:970.

Case C-434/16 Peter Nowak v Data Protection Commissioner, [2017], Judgment of the Court, ECLI:EU:C:2017:994.

C-210/16 - Wirtschaftsakademie Schleswig-Holstein, [2018], Judgement of the Court, ECLI:EU:C:2018:388.

C-25/17 Jehovan todistajat — uskonnollinen yhdyskunta,[2018], Judgement of the Court, ECLI:EU:C:2018:551.

Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV. [2017], Judgement of the Court, ECLI:EU:C:2019:629.

Case C-673/17, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände –Verbraucherzentrale Bundesverband e.V. [2019], Judgement of the Court, ECLI:EU:C:2019:801.

Joined Cases C141/12 and C372/12 YS (C141/12) v Minister voor Immigratie, Integratie en Asiel, Minister voor Immigratie, Integratie en Asiel (C372/12) [2014] Judgement of the Court, ECLI:EU:C:2014:2081.

Opinion of Advocate General Tizzano 19 September 2002, Case C-101/01, Bodil Lindqvist. ECLI:EU:C: 2002:513

Opinion of Advocate General Jääskinen delivered on 10 July 2014, C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, ECLI:EU:C:2014:2072.

Opinion of Advocate General Mengozzi delivered on 1 February 2018, C-25/17 Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta, ECLI:EU:C:2018:57

Opinion of Advocate General Bobek delivered on 19 December 2018, Case C-40/17 Fashion ID, ECLI:EU:C:2018:1039.

Opinion of Advocate General Bot delivered on 24 October 2017, C-210/16 - Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2017:796.

Opinion of Advocate General Szpunar delivered on 21 March 2019, Case C-673/17 Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

EU Documents

Article 29 WP _Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

_ Guidelines on consent under Regulation 2016/679.

_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

_Guidelines on transparency under Regulation 2016/679.

_2013 Statement of the Working Party on current discussions regarding the data protection reform package- Proposals for Amendments regarding exemption for personal or household activities.

_ 1/2010 Opinion on the concepts of "controller" and “processor” Adopted on 16 February 2010.

_ 5/2009, Opinion on online social networking’.

_ 06/2014 Opinion on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

_ 8/2014, Opinion on the on Recent Developments on the Internet of Things’.

_ 15/2011 Opinion on the definition of consent Adopted on 13 July 2011.

Council of the European Union, 2020. Shaping Europe's Digital Future- Council Conclusions (9 June 2020).

European Commission, 2015 “Eurobarometer Qualitative study - “Public opinion on future innovations, science and technology” - Aggregate Report”, June 2015.

_2018a “Commission Staff Working Document Impact Assessment 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.

_ 2018b “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}.

_2018c “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, Coordinated Plan on artificial intelligence” (COM (2018) 795 final).

_2019 “The General Data Protection Regulation Special Eurobarometer 487a”, June 2019.

_2020a “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, A European strategy for data, COM/2020/66 final.

_2020b “White Paper On Artificial Intelligence - A European approach to excellence and trust”, COM(2020) 65 final.

European Economic and Social Committee, 2017. Artificial intelligence – The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society. INT/806 – EESC-2016-05369-00-00-AC-TRA (NL) 1/13

EDPB, 2020a, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020.

EDPS _2012a “Opinion of the European Data Protection Supervisor on the data protection reform package”, (7 March 2012).

_ 2012b “Opinion of the European Data Protection Supervisor on the Commission's Communication on Unleashing the potential of Cloud Computing in Europe”, (16 November 2012).

_2016 “Artificial Intelligence, Robotics, Privacy and Data Protection. Room document for the 38th International Conference of Data Protection and Privacy Commissioners”, (October 2016).

_ 2019 “Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725”, (7 November 2019).

_2020b “opinion 3/2020 on the European strategy for data, 16 June 2020.

European Parliament, 2015 resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics procedure 2015/2103(INL).

_ 2016 Scientific Foresight Study Ethical Aspects of Cyber-Physical Systems, Science and Technology Options Assessment Panel, June 2016.

_ 2018 resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI))

_ 2020 Committee on the Internal Market and Consumer Protection Draft Motion for a Resolution on Automated decision-making processes: Ensuring consumer protection, and free movement of goods and services (2019/2915(RSP)), 21.01. 2020.

High-Level Expert Group on Artificial Intelligence (HLEGAI), 2019a. “A definition of AI: Main capabilities and scientific disciplines”, April 2019.

_2019b. “Ethics Guidelines for Trustworthy AI”, April 2019.

EPRS Documents

Bentley, P. J., Brundage, M., Häggström, O., and Metzinger, T. (2018) “Should we fear artificial intelligence?” European Parliament Directorate-General for Parliamentary Research Services.

Boucher, P. (2019) Why artificial intelligence matters, European Parliamentary Research Service Scientific Foresight Unit (STOA), PE 634.421.

Delponte, L (2019). European Artificial Intelligence (AI) leadership, the path for an integrated vision, Study for the Committee on Industry, Research and Energy, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, European Parliament, Brussels.

Dolic, Z., Castro, R., Moarcas, A., (2019). 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.

Przegalinska, A. (2019). State of the art and future of 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.

Sartor, G. (2019). Artificial Intelligence: Challenges for EU Citizens and Consumers. 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, 2019.

_2020a. 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.

_2020b. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. Panel for the Future of Science and Technology.

Szczepański, M. (2019) EU Legislation in Progress 2021-2027, EPRS Members' Research Service PE 628.231 – February 2019 EN Digital Europe programme

Miscellaneous

Access Now (2018). Human Rights in the Age of Artificial Intelligence.

_ (2019). Two years under the GDPR: An Implementation Progress Report.

AGCOM (Autorita per le Garanzia Nelle Communicazioni) (2017). Big Data: Interim Report in the context of the joint inquiry on “Big data” launched by the AGCOM deliberation No. 217/17/CONS.

AGID (the Agency for Digital Italy). White Paper on Artificial Intelligence at the service of citizens. March 2018.

AI voor Nederland, AINED, Oktober 2018.

Brief van de Minister voor Rechtsbescherming Aan de Voorzitter van de Tweede Kamer der Staten-Generaal Den Haag, 8 oktober 2019 p.5.

Bughin, J., Seong, J. M., Hämäläinen, J., Windhagen, E., Hazan, E. (2019). 'Notes from the AI frontier: Tackling Europe's gap in digital and artificial intelligence', McKinsey Global Institute, McKinsey&Company.

Cavoukian, A. (2010) "Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", Information and Privacy Commissioner of Ontario.

CoE, (2018), Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory IMplications, Committee of Experts on Internet Intermediaries. Council of Europe study, DGI (2017) 12.

Farrell, H., Newman, A. (2016) "The Transatlantic Data War: Europe Fights Back against the NSA", Foreign Affairs VO - 95. Council on Foreign Relations, Inc.

FMEAE (Finnish Ministry of Economic Affairs and Employment), 2017, "Finland's Age of Artificial Intelligence: Turning Finland into a leading country in the application of artificial intelligence", Objective and recommendations for measures.

_2019 "Finland's Age of Artificial Intelligence: Turning Finland into a leading country in the application of artificial intelligence" Final report of Finland's Artificial Intelligence Programme.

Fosch-Villaronga, E. (2017). 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.

Google, Methods and systems for robot personality development, U.S. Patent 8996 429 B1, 31 March 2015.

Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence, Council of Europe/European Court of Human Rights, 2019.

House of Commons, (2018) Algorithms in decision-making, Fourth Report of Session 2017–19.

House of Lords (2018) AI in the UK: ready, willing and able? Report of Session 2017–19. London: House of Lords Select Committee on Artificial Intelligence. (2018, April 16).

ISO 8373:201 Robots and robotic devices – Vocabulary

ISO 13482:2014 Robots and robotic devices — Safety requirements for personal care robots

Istituto Italiano di Tecnologia, (2018). 2018-2023 Strategic Plan.

Information Commissioner's Office, (ICO) (2017) Big data, artificial intelligence, machine learning and data protection.

_2019, Project explAIn: Interim report.

_2020, Explaining decisions made with AI.

ITU Security, Infrastructure and Trust Working Group: Big data, machine learning, consumer protection and privacy, International Telecommunication Union, 2018.

Küzeci, E., (2010). Kişisel verilerin korunması/Data Protection. Doktora Tezi. Ankara Üniversitesi, Sosyal Bilimler Enstitüsü.

Leroux, C., Labruto, R., Boscarato, C., Caroleo, F., Günther, J.P., Löffler, S., Münch, F., Beck, S., May, E., Huebert-Saintot, C., de Cock Buning, M., Belder, L., de Bruin, R., Bonarini, A., Matteucci, M., Salvini, P., Schafer, B., Santosuosso, A., Hilgendorf, E. (2012) Suggestion for a green paper on legal issues in robotics. euRobotics, The European Robotics Coordination Action, 7th Framework Programme.

Leslie, D. (2019). 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. https://doi.org/10.5281/zenodo.3240529.

Ministry of Economic Affairs and Climate Policy, (2018). Dutch Digitalisation Strategy June 2018.

National Research Council, (2012). Intelligent Human-Machine Collaboration: Summary of a Workshop. Washington, DC: The National Academies Press. https://doi.org/10.17226/13479.

Óbuda University (2017). Cutting Edge Robotics Research in Hungary, Antal Bejczy Center for Intelligent Robotics, Budapest.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980.

Perrault, R, et. al. (2019). “The AI Index 2019 Annual Report”, AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA.

Reinsel, D., Gantz, J., Rydning, J. (2018) “Data Age 2025: The Digitization of the World from Edge to Core”, IDC.

Ribera, M., & Lapedriza, À. (2019). Can we do better explanations? A proposal of user-centered explainable AI. IUI Workshops.

Robotics in the Netherlands, (n.d.). Shadana Innovation Management and Consultancy report prepared for the State Agency for Enterprising.

ROSE consortium, (2017). Robotics in Care Services: A Finnish Roadmap, Retrieved from: http://roseproject.aalto.fi/images/publications/Roadmap-final02062017.pdf

Stats NZ (2018). Algorithm assessment report. Retrieved from: https://data.govt.nz/use-data/analyse-data/government-algorithm-transparency

Talty, S. (2018) What will our society look like when artificial intelligence is everywhere? Smithsonian magazine, https://www.smithsonianmag.com/innovation/artificial-intelligence-future-scenarios-180968403/

United Nations (2017) Report of COMEST on Robotics Ethics, SHS/YES/COMEST-10/17/2 REV, 14 September 2017

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., West, S.M., Richardson, R., Schultz J., Schwartz, O. (2018). AI Now Report 2018, AI Now Institute.

Appendix

(Survey questions referred to the experts)

Proposed Case Study for PhD Project

A. Preliminary questions (before the participant reads the case study)

1. Do you think that current European data protection legislation is addressing issues related to Artificial Intelligence sufficiently?

2. What kind of "data breaches" would you identify as being likely with AI technologies?

3. Have you ever experienced a case (either as an expert or a lawyer) which refers to AI technologies, or at least algorithmic decision making? Do you know any (national) court case(s) related to this topic?

4. What is your overall opinion regarding current discussions regarding defining data controllers/data processors in AI technologies? (This refers to the question of liability)

B. Questions to be asked to the participant after the case study has been presented

General Questions

1. What is your overall opinion about the scenario?

2. What do you like most about this scenario? List (at most) your top 3 aspects (if any).

3. What did you not like about this scenario? List (at most) your top 3 aspects (if any).

4. Do you think the type of technology referred to in the scenario could possibly be achieved in the near future (say next 10-20 years)? Yes/No/Don't know

5. What further problems or risks regarding personal data protection might occur within the scenario? (E.g. robot is stolen/hacked, the user is deceased…)

6. Who would be the relevant "persons" in the scenario? What would be their responsibilities/liabilities, according to you?

7. Would your interpretation of the scenario differ if the data subject was an elder (or otherwise vulnerable) person?

8. To which national or CJEU case(s) would you refer in order to resolve the relevant legal issues in this scenario? (optional)

9. If such a case is referred to the national court, how would you defend the company? (claims and evidences)

10. If the case were referred to the national court in your country, how would Julia and/or

her son be defended? (claims and evidences)?

11. To what other legislation would you refer in order to interpret this case, besides GDPR? (if any)

12. Does the “right to explanation" make sense in this scenario where the machine already made a decision about the data subject? (opinion)

13. Could the GDPR prevent data controllers to create robots persuading the users to disclose

information about themselves? (natural interaction, constant interruption, or silence)

14.What would be your final decision regarding the case, if you were to act as a decision maker? (who is liable and what might be the sanction)

15. Could you propose any solution(s) in order to prevent such scenarios from occurring? Do you think the GDPR rules should be or could be updated to prevent or avoid such situations?