Application of the General Data Protection Regulation on Household Social Robots

Synopsis of the 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

Table of Content

Blood of a robot is the data; brain of a robot is the algorithm.

Background of the Dissertation

Artificial Intelligence (AI) is probably one of the most popular topics of the last five years in the academia. The topics was discussed more or less almost in any field creating an opportunity for the researchers to conduct interdisciplinary researches. AI and robots today appear in healthcare, transportation (including interspace transportation), construction, goods and services delivery, financial services, education, in short, in every field of life. Indeed, there is a sound reason for that. AI-enabled health care technologies could perform in prediction of diseases better than the traditional tools and could reduce the clinical errors at the clinics using AI compared to the clinics do not. 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 just 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 available cheap hardware placed in markets, as well as the improvements in 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 every people's life.

First of all, we need to clarify the terminology used throughout the dissertation to give a clear understanding on the concept of the topic. During the literature review, we detected different approaches focusing on the distinction between, as well as the uniformness of the terms AI and robots. The dissertation did not differ AI and robots, the readers of this booklet shall read the terms AI and robots interchangeably. We are aware of the fact that both of the technology's blood is data, especially personal data in case of personal use, and algorithms are the brain of these artificial entities. Robots, furthermore, raises extra concerns on the right to data protection, as will be presented during the booklet.

Indeed, we also need to clarify what type of robot we took into consideration during the analysis. There are several types of robots classified mainly under two main categories: industry and service robots. This work focuses on service robots in general, but social robots specifically. 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. 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 Boston Dynamics produce are developed and tested for military purposes, rather than personal ones. Self-driving cars and drones are 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 need. The robot in the project is being developed with Machine Learning (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 robot, an open-source low-cost robot that could navigate in physical spaces supported with AI navigating without needing a map. Although the full appearance of social robots at 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. 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, according to the forecasts made in several pieces of literature. This 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 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. 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 this dissertation could be the starting points.

Since the risks have been identified as both in this work and in the literature, the legal academia and the 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. We reviewed the EU-legal literature on AI, meaning, the research papers done by or for the European Parliament and European Commission policy papers to get the first insight on the current issues and regulative approaches in the EU. These papers, in summary, call the related institutions, as well as the MS, to understand the challenges with AI technology as well as specific to fundamental rights point of view. They draw the attentions to the importance of identifying specific safeguards related to the use of AI tools. Such safeguards should highlight the ethical, social, and legal aspects and needs of the topic, and could even raise new applicable rules to avoid legal uncertainty. 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). All in all, we assess the applicability of the General Data Protection Regulation (GDPR) on this very specific technology.

Identification of Research Tasks and Motivation

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.

A novelty of this dissertation is vested on the aspect that it is testing a social robot's legal consequences precisely on data protection topic which has not yet been examined in the legal academia. 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 before starting a policy-making procedure. It also brings a tangible roadmap to deal with the questions referred within the legal and technical academia. Through the analysis made in the dissertation, we aimed to show possible practical/application 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.

The output of the present dissertation 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.

Data Collection and the Applied Methods

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 subjected to this dissertation; any researcher attempting to use forecasting methods should first check the prior works and test the applicability of the method in own work. There are several pieces of literature referred in the dissertation regarding the methodology, but considering the fact that the present booklet shall not include them all, we would like to mention one of them that 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.

Futures Research Methods

An international conference called WeRobot focusing only on robots and law (Robolaw) related issues has been organized by one of the most famous Robolaw scholars, Prof. Ryan Calo in his joint work entitled "Taking Futures Seriously: Forecasting as Method in Robotics Law and Policy" implemented the method accordingly. The paper proposes an appropriate method for shaping the Robolaw, stating that we could prevent the unintended consequences of future legal problems with the help of a foreword thinking way. 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 Human-Robot Interaction researchers also use this method frequently). The authors of the work 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. Later, we used the interview method and comparative analysis of the expert opinions that will be explained further.

We need to shortly mention about the design fiction and the scenario planning methods to ensure the understanding of these-not much practices in law-methods. The design fiction method is heavily used in different law-related fields, such as ethics. The famous Trolley Problem 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", 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 that is also strongly referred also 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 the Article 25 of the GDPR, the design fiction method is a sufficient method to analyze the questions referred to in this work.

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. They have been used for forecasting and by policy analysis researchers for more than 60 years. The method aims to connect present issues with the future through cause and effect links. The intention behind the scenarios is to assist either policy-makers or decision-makers to act now instead of acting later under emergency. This dissertation has a very 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.

One may ask whether such methods are sufficient for an academic scientific work and may fall on the illusion of what the Sci-Fi literature has been presenting. The items are shown as part of Sci-Fi literature evidentially become real, and become an ideal tool for the industry. The relationship

between scientific researches and the Sci-Fi has evolved in a way that today, the former comes after the latter. Julian Bleecker, a team member of the Near Future Laboratory where design fictions are turned out to be a prototype in the industry says, that "the science happens in between the fact and the fiction", pointing out the fact that it may not always easy to observe the difference between the real science and the fictional one. 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. 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.

Scenario in the Dissertation

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 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. The scenario focused on an everyday social robot developed with a combination of ML methods such as Reinforcement Learning technique, and being used at the household to assist the user for her to overcome Alzheimer onset. The robot, called Robinsan, collects and processes personal data in an autonomous way. Robinsan causes such actions that make us question the validity of the consent rules, natural person's possible liability, rules regarding the algorithmic decision making (ADM), and the other questions referred related to the Hypothesis below. Once the initial scenario was ready, it was shared with seven scholars for their evaluation based on a conversation. 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 the several questions placed in the questionnaire.

Interviews

To ensure the validity of the fictional case and to collect necessary data, this work practices also interview method 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. After choosing the location, the following criteria were identified when choosing the experts who:

- Currently work at a law firm or an institution taking a role in the implementation or interpretation of the GDPR (National Supervisory Authority, NSA),
- 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 it is the right approach considered in the literature. 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 there is an unclear situation. This act also allowed us raising some new questions, paving a new way of pointing to new aspects of the scenario.

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.

A comparative approach adopted on analyzing the experts' opinions influencing their decision-making helped us to experience their worlds and critiques 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, 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). The comparative method in this work is scientific (or a theoretic) one, rather than a legislative one, 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.

Literature Considered

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 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.

Research Questions and Hypotheses

This work focuses on the practical, legal, and technical problems arising from the use of personal social household robots in which the GDPR designed in a technology neutral sense. These problems, as grouped below, was extensively analyzed and are 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.
- 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.
- 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").

- 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.

Overall presentation of the dissertation

The dissertation consists of seven main chapters. Each chapter focuses on the technical and legal foundations of the research questions. Chapter I presents the Introduction section where the current standing point of the EU towards regulating AI technologies was described with the help of EU policy papers. Then, the methodology used, the data evaluation technique, and the literature review conducted during the preparation of the work was explained. Chapter II steps into the dissertation's topic in which the historical development of right to data protection in Europe, as well as the related legislation and the related articles within that legislation were presented. Technological development and the new protection challenges reported at the end of this chapter connects the work to the the third chapter. Chapter III focuses on the terminological discussions that related to the definition of AI and robot by pointing also some of the technical foundations of these technologies. It also gives the definitions adopted by the EU institutions or agencies, therefore draws the boundary of the legal definitions. Chapter IV slightly enters into the territorial focus points of the work meaning that a descriptive analysis regarding the AI and robotics in the EU, Hungary, Italy, the Netherlands, and Finland was conducted. Chapter V comprehensively evaluates the problems related to AI technologies and the GDPR, and does this under two Sections. Section 1 focuses on the conceptualization of the problems based on the definitions in the GDPR and discusses the related concepts to the robotics such as the personal data in the GDPR, the data disclosures, profiling, automated decision making, algorithmic decisions, the data subjects and the data controllers. Section 2 presents the practical problems, such as, defining the right legal bases for operation household robot. This section also predicts that the rules and principles embedded in the GDPR (e.g., purpose limitation, transparency, informing obligation, etc.) may not be well applicable to the AI because of their Unpredictable by Design character. Chapter VI provides the two analyses based on the presented problems: the first analysis focuses on our own analysis and the second one presents the expert opinions on the constructed scenario. This chapter elaborates the assessment of the research questions. Chapter VII concludes the dissertation work and raises few practical solutions to tackle the questions related to applicability of the GDPR on social robots.

Findings

First analysis

As mentioned before, the first analysis focuses on the interpretation of the scenario based on the GDPR and in accordance with the case law of the CJEU. As a result of this analysis, the resources point the difficulty of balancing the other fundamental rights with the right to data protection

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 CJEU 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 CJEU 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, obtaining consent, or creating grounds for withdrawing consent. This rule may be interpreted as people recorded by Robinsan (or a social robot, with a general term) considered to be falling in the public space since they are not belonging to the household, even if the other people except than the main user is subjected to the evaluation. Either any NSA 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, the main user would certainly be under the 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

Further, it is crystal clear for data controllers to obtain the consent of the main user of a social robot, but also other people about processing their data automatically recorded by the robot once they entered into the main user's house. For example, if Robinsan's company plans to use such data for various, e.g., commercial purposes, the Company must obtain a separate consent. If the main user people entering her home to accept the robot around them, then she 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. In this case, 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 seems challenging.

On the other hand, 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 the main user's treatment, and still they receive the services, then it may be considered against the granularity element since the service includes more purposes than the original ones. 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.

In conclusion, 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.

Second analysis

Based on the expert feedback on the scenario presented in the work based on the questionnaire, the scenario 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.

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 some of the experts verified, the bigger problem with the application of the GDPR that is the visible tendency in most of the National NSA'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 NSAs are more actively preparing agendas and working on the AI and ADM, while there is no such preparation observed in the Italian and Hungarian NSAs.

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 efficiently work. 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 the main user to obtain 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.

Proposed solutions were constructed on the findings presented above and mentioned comprehensively in the end of the dissertation.

List of Relevant Publications

1. Gültekin Várkonyi, G.; Varadi, Sz.; Kertesz, A. Legal Issues of Social IoT Services: The Effects of Using Clouds, Fogs and AI In: Taha, Mohamed Hamed N.; Khalifa, Nour Eldeen M.; Bhatnagar, Roheet; Hassanien, Aboul Ella - Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications Springer International Publishing, (2020) pp. 123-138ç, 16 p.

2. Gültekin Várkonyi, G. ; Sz., Varadi ; A., Kertesz Legal Aspects of Operating IoT Applications in the Fog In: Rajkumar, Buyya; Satish, Narayana Srirama (eds.) Fog and Edge Computing: Principles and Paradigms Hoboken (NJ), United States of America : John Wiley & Sons, (2019) pp. 411-432. , 22 p.

3. Gültekin Várkonyi, G. Consent Mechanism in the Life with Social Robots, European Review of Public Law 31 : 1, p. 111, (2019).

4. Gültekin Várkonyi, G. Operability of the GDPR's Consent Rule in Intelligent Systems: Evaluating the Transparency Rule and the Right to Be Forgotten In: Andrés, Muñoz; Sophia,Ouhbi; Wolfgang, Minker; Loubna, Echabbi; Miguel, Navarro-Cía. Intelligent Environments 2019: Workshop Proceedings of the 15th International Conference on Intelligent Environments, Amsterdam, Netherlands : IOS Press, (2019) pp. 206-215. , 10 p.

5. Gültekin Várkonyi, G; Kertesz, A. ; Varadi, S. Privacy-awareness of users in our cloudy smart world. In: 2019 4th International Conference on Fog and Mobile Edge Computing, FMEC 2019 (2019) pp. 189-196. Paper: 8795310 , 8 p.

6. Várkonyi Gültekin, G. Life after the GDPR: Dreaming of a Uniform Application In: Várkonyi Gültekin, Gizem; Sulyok, Márton (eds.) Life After the GDPR: Good DataProtection Rules and Prospects for the Future Szeged, Hungary : Szegedi Tudományegyetem Állam- és Jogtudományi Kar Nemzetközi és Regionális Tanulmányok Intézete (SZTE ÁJK NRTI), (2019) pp. 69-83, 15 p.

7. Dogaru, Tatiana-Camelia ; Várkonyi Gültekin, G., National Paths on implementing EU GDPR: a legal approach CURIERUL JUDICIAR 11 : Supliment Paper: 15 (2018).

8. Gültekin Várkonyi, G. International Personal Data Transmission: European Union Approach. In: Fejes, Zsuzsanna (eds.) Jog határok nélkül Szeged, Hungary : Szegedi Tudományegyetem Állam- és Jogtudományi Doktori Iskola, (2018) pp. 101-112. , 12 p.

9. Gültekin Várkonyi, G., Szç, Varadi; A, Kertesz. Law and IoT: How to see things clearly in the Fog. In: Institute, of Electrical and Electronics Engineers (eds.) 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC) Piscataway (NJ), United States of America : Institute of Electrical and Electronics Engineers (IEEE), (2018) pp. 233-238, 6 p.