DOI 10.26521/profuturo/2020/4/9570

Gültekin Várkonyi Gizem*

A Case Study on the Interaction Between the General Data Protection Regulation and Artificial Intelligence Technologies

Esettanulmány az általános adatvédelmi rendelet és a mesterséges intelligencia technológiák kölcsönhatásáról

Abstract

This paper presents a general overview of the problems regarding the regulation of artificial intelligence (AI) raised in the official published works of the European Union (EU) and interprets these problems from the perspective of the Hungarian experts as a case study. Even though a new regulation on AI has already been proposed at the EU level, the paper evaluates specific rules and principles regarding data protection since data is the lifeblood of AI systems and the protection of such data is a fundamental right enshrined in the EU legislation via the General Data Protection Regulation (GDPR). The result of the study shows that the application of the GDPR on AI systems in an efficient and uniform way might be at stake since different outputs were generated by the experts to the same legal questions deriving from a scenario presented.

Keywords: *data protection, artificial intelligence, GDPR, future research, data controller, consent*

Absztrakt

A tanulmány az Európai Unió (EU) hivatalosan publikált dokumentumaiban felvetett, a mesterséges intelligencia (MI) szabályozásával kapcsolatos problémák általános áttekintését adja, és ezeket a problémákat a magyar szakemberek szemszögéből esettanulmányként mutatja be. Annak ellenére, hogy uniós szinten már javasoltak egy új, a mesterséges intelligenciáról szóló rendeletet, a cikk az adatvédelemre vonatkozó konkrét szabályokat és elveket értékeli, mivel az adatok jelentik a mesterséges intelligencia-rendszerek lelkét, és az ilyen adatok védelme az uniós jogszabályokban az általános adatvédelmi rendelet (GDPR) által rögzített alapvető jog. A tanulmány rámutat, hogy az MI-rendszerekben a GDPR hatékony és egységes alkalmazása problémás lehet, mivel a szakértők a felvázolt szituációra vonatkozó jogi kérdésekre eltérő válaszokat adtak.

Kulcsszavak: *adatvédelem, mesterséges intelligencia, GDPR, jövőkutatás, adatkezelő, hozzájárulás*

Regulation of AI[1] has increasingly become a salient topic both in the legal literature and in the EU policy-makers' agendas in the last couple of years, due to

* Gültekin Várkonyi Gizem, PhD, junior research fellow, University of Szeged Faculty of Law and Political Sciences International and Regional Studies Institute; e-mail: gizemgultekin@windowslive.com.

[1] Based on the EU policy documents and the expert opinions analyzed in this paper, the terms artificial intelligence (mostly understood as a software installation) and robotics (that is the embodied artificial intelligence) are being used interchangeably.

the developments encountered in the engineering field, accessibility of the relevant equipment and the availability of data. Data protection is one of the concerned areas reflected in the studies conducted by the European Parliament and the European Commission owing to the fact that the AI technologies could lead 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 their users through different Machine Learning (ML) techniques in order to customize services in line with the user's needs. While autonomous learning and autonomous decision-making maximizes the robots' operability, questions related to designing data protection friendly robots protecting both their user's and the others' privacy interacting with robots have also came into the picture, since they could contribute to further learning processes of the robots. Questions regarding liability and responsibility as well as exercising the rights of data subjects seem the most urgent to be answered. Although one of the aims of the GDPR[2] is to take proactive steps to reduce the risks arising from the use of robots in the personal sphere, it may alone not cover all the aspects of this specific technology which is to be built on people's trust. Data protection friendly robotic applications could better ensure people's trust once they could be built in the current EU legislation via a clear de lege referenda approach set forth in line with the voice of the EU Member States. In order to foresee the possible problems that could arise from the application of specific legislation on a specific technology like AI, forecasting methods combined with expert interpretations collected via interviews could be useful. Such a method could help the policymaker to design better legislation, if the aim is not to be late in giving immediate answers to the questions generated by emerging technologies. This paper aims to contribute to the current efforts of the European Parliament (EP) and the European Commission (EC) on the regulation o AI and robotics applications from the data protection point of view, and also to help Hungarian policy makers understand what to take into account in case they are to initiate a guideline or policy papers in Hungary.

The present paper consists of two sections. The first section gives an evaluation of the chronological summary of the papers generated by or upon the request of the EP and the EC. Evaluation of these papers will serve to understand the problems specific to the AI technologies from the data protection point of view, and furthermore from the EU's point of view. The second section reports the Hungarian experts' opinions specific to the regulation on data protection in AI technologies that might be an input contributing to the works of either the EU or Hungarian policy makers. It is true that already a regulation on AI technologies was proposed in April 2021,[3] however, bearing in mind that it lays down general rules based on high-risk AI that could operate better with applicable data protection rules, evaluation of the possible future risks gains even more importance. The expert opinions were collected through

[2] 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) [2016] OJ L 119/1.

[3] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final.

standard pre-set survey questions based on a futuristic scenario. The state of the art data collection method will be presented in the beginning of the second section. The connection between the first and the second section can be seen from the mere fact that the EP also referred to experts' opinions often in its published works, in order to have an insight into an unknown topic, and the present paper does so via the Hungarian experts' opinions. Additionally, Hungarian experts' opinions collected through the help of a novel scenario could contribute to identifying new aspects of the topic to be taken into account by either the national authorities or the EU policy makers.

1. Problem Statement and the Chronological Summary of the EU Policy Papers

The EU has been putting significant effort into understanding AI and robotics technologies in strategical, ethical, and legal meanings. Data Protection and privacy related issues have been the very first topics where the EU was called to review the current legal rules through the several policy or research papers generated by or upon the request of the EU Institutions, which took place particularly heavily during the last three years. Following this kick-off, the EP's special interest has continuously increased up to the present time, consisting mostly of the EU-AI literature supported with by a few yet significant policy papers generated by the EC (also assisting the proposed AI regulation). The content of these papers could draw a clear picture for anyone looking for the problems specific to the intersection of the AI and data protection topic.

1.1. European Parliament Working Papers

The very first attempts towards identification of the problems related to regulation of AI and robotics technologies in the EU were made by the EP. A motion for a resolution in 2017[4] discussing the civil liability of robotics addressed three problems specific to data protection in robotics: robot surveillance, unclear liability distribution, and ineffective consent implementations appearing during the use of robots. Following this kick-off, several working groups were formed under the EP to analyze the questions in-depth, serving as an assistance to the EP to understand the concept better. In 2016, a report was prepared for the EP[5] indicating the very first concerns about the home-care robots, such as healthcare robots, that could comprehensively (i.e. illegally) collect and process personal data. Furthermore, algorithmic transparency, the risks arising from using a robot for household activities, questions of data ownership and data sharing, and the relationship between data controllers and data

[4] European Parliament Resolution 2015/2103(INL) of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics procedure [2018] OJ C 252/239, 19.

[5] European Parliamentary Research Service Scientific Foresight Unit, Ethical Aspects of Cyber-Physical Systems Scientific Foresight Study (PE 563.501 2016) 1, 10.

processors were also identified as challenges within the document. Meanwhile, the traditional International Conference of Data Protection and Privacy Commissioners meeting in 2016 was dedicated to the AI and privacy challenges pointing out the need for identifying implementation rules for transparency and explainability rules on AI systems.[6]

Due to the criticism that the EU's data protection regime was holding the EU back from having a strong AI position in the world[7], the EP advocated taking immediate legislative steps to react.[8] Essentially, right implementation on obtaining an unambiguous and informed consent compelling the AI developers[9] due to AI's learning and autonomous features were the highlighted themes. Purpose limitation and data minimization rules were discussed due to the difficulty of their complying with AI practices, placing the burden on the shoulders of the data controllers, as noted in a later work.[10]

Another report released in 2019[11] gave specific examples on chatbots and social robots and drew attention to the success behind their application from the point of view of their ability to engage people interacting with them. While such interaction may cause more data disclosures by the data subjects and invalidate the consent practices, the report recommended the High-Level Expert Group on Artificial Intelligence (HLEGAI) to review the GDPR and as to whether it could respond to the issues arising from AI and algorithmic decision-making services. The call was the first (and probably the last) for such a revision. Reinforcing the statements in the report, another study[12] gave a specific overview on the risks arising from the evaluation of personal data in AI systems. This work evaluated only the GDPR and AI related questions and reached the conclusion that comprehensive profiling leading extraction of new personal data and data repurposing should be evaluated in a social context, which the present work aims to do.

[6] European Data Protection Supervisor, *Artificial Intelligence, Robotics, Privacy and Data Protection* (Room document for the 38th International Conference of Data Protection and Privacy Commissioners, October 2016) 1, 9.

[7] Laura Delponte, *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, 2019) 1, 16; Zrinjka Dolic, Rosa Castro, Andrei Moarcas, *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, 2019) 1, 8–12.

[8] European Parliament Resolution 2018/2088(INI) of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics, [2020] OJ C 449/37, para. 110.

[9] ibid., para. 129.

[10] Giovanni Sartor, *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) 1, 5.

[11] Aleksandra Przegalinska, *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, 2019) 1, 6.

[12] Giovanni Sartor, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (Study for the Panel for the Future of Science and Technology, European Parliament, 2020) 1, 3 para. D.

The final study to be mentioned under this title is the one prepared in June 2020[13] which reported issues only about the relationship between data, personal data, and AI technologies by evaluating the principles and rules applicable in the GDPR. The most important contribution of the study was where AI technologies were evaluated as they could have such technical settings that may cause complexity in understanding, inexplicability and unpredictability hindering the transparency principle which is one of the principles which data controllers are bound to comply with. It is an important aspect to note as it could hinder the consent practices available currently, as will be explained in the summary of this section.

1.2. European Commission Policy Papers

The EC's involvement with policy planning towards regulation of AI technologies resulted in significant policy papers during the last two years. In the year 2018, the EC published the "EU AI strategy"[14] that was one way to understand how the EU analyzed the differences and similarities, as well as the gap between the MS in terms of their AI readiness, including ethical and legal readiness. In the pillar of the ethical and legal framework, the AI strategy identified data protection and privacy issues as challenges to be tackled based on strict rules. Indeed, HLEGAI was set up by the EC which was a significant step towards a possible AI regulation, together with creating a chance for analyzing the questions regarding data protection. The HLEGAI published "ethics guidelines"[15] referring to seven requirements for establishing human-centric AI that are complementary to each other. One of the requirements referred to privacy and data governance supported with such requirements that are directly connected with it, such as transparency, fairness and accountability.

The AI strategy was accompanied by the European data strategy,[16] the aim of which was to raise the EU to a world leader position in terms of data innovation in any areas such as healthcare, transportation, banking, and education. To reach this aim, it was clearly stated that the rules and enforcement of the rules should have also ensured personal data protection. The problems stated in relation to the data protection specific cases were, expectedly, much similar to the ones reported in the EP literature. Furthermore, lack of standards and tools preventing data subjects to exercise their rights in a simple way, together with a lack of necessary data literacy to understand the complexity of AI, were noted.[17]

The last document published by the EC was the White Paper on Artificial Intelligence[18] containing policy options to ensure trustworthy development of AI in Europe

[13] Aimee van Wynsberghe, *Artificial intelligence: From ethics to policy* (Study for the Panel for the Future of Science and Technology, European Parliament, 2020).

[14] Commission 'Artificial Intelligence for Europe' (Communication) COM(2018) 237 final.

[15] HLEGAI, 'Ethics Guidelines for Trustworthy AI' 2019.

[16] Commission, 'A European strategy for data' (Communication) COM/2020/66 final.

[17] ibid.

[18] Commission, 'White Paper on Artificial Intelligence – A European approach to excellence and trust' (Communication) COM (2020) 65 final.

while benefitting from the value of the data excellently. Under the problem definition title, the paper reported the risks for fundamental rights including personal data and privacy protection, and principle of non-discrimination at the first place. The risks were assigned to the human oversight, the design of AI and the autonomous and black-box[19] nature of machine learning that complicate the explainability. In the summary below, all the problems and risks highlighted by the EP and EC papers will be explained in light of the related GDPR rules and will be integrated into the problem statement.

1.3. Summary and Evaluation

According to the papers summarized above, specific rules regarding data protection and privacy are (or should be) an integrated part of the EU AI legislation. It is easily understandable that either the newly proposed regulation or during practicing GDPR the risks and problems stated in the policy papers will be faced, and need to be solved beforehand, not just when the problem actually occurs. Overall problems in AI technologies specific to data protection and privacy are:

(1) AI and robotic applications may cause mass surveillance and profiling, which are some of the risks arising from use of robots. Particularly personal home-care robots, for example, may comprehensively collect and process personal data as a result of profiling activity and this is strictly prohibited in the GDPR. According to the Article 5 of the GDPR, personal data should be processed lawfully, prohibiting surveillance leading illegal data processing and Article 12 of the GDPR gives data subjects the right not to be subject to a decision based solely on automated processing, including profiling that is actually the basic rule of AI when collecting data. AI systems' way of working logic is based on massive collection and evaluation of data which ends with a generation of an output, mostly leading to personal aspects of the data subject being evaluated. Even though the data used for training purposes may not be personal one, there is a strong probability for reaching personal outputs as a result of applying the algorithmic evaluation on personal cases. This is due to AI's ability to extract new meanings in the given cases. Technical foundations of AI enabling this technology to perform autonomous decisions, together with profiling, new data about data subjects might possibly be extracted which is contrary to the purpose limitation and data minimization rules, as they are the basic principles referred to in the Article 5 (b) and (c) of the GDPR. Either the data collection and purposes or the generated outputs may not be limited to the foreseen processing purposes by the data controller.

(2) 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. This may pull the natural persons as

[19] The term, very basically, refers to the difficulty in explaining what exact data the algorithm processed and what methods or rules were used in processing to reach a certain output is unknown even to the designer or programmer of the system due to its technical complexity.

users into the data controller paradox which refers to the complexity of identifying the responsible person in case privacy infringement is detected. Liability questions rise at this point, where the system reaches an output autonomously, making it difficult to identify how the system evaluated the data to reach that output. Anyone contributing to the learning phase of a robot, e.g. the programmer or the user, might carry a degree of responsibility in this case. Although identifying natural persons as data controllers is not a desirable solution in real cases, there still is a probability at least in terms of their responsibility operating an AI at their households.

(3) Technical complexity and the black-box nature of the algorithmic assessments may hinder the transparency and explainability principles which are relevant to data repurposing, unforeseeable system functionality, and finally, complex data controller relationships, which may prevent data subjects from exercising effective consent implementations, if not making it impossible to give informed and unambiguous consent. In use cases where an individual interacts with a robot based on consent as a legal basis in line with Article 6 of the GDPR, conditions of obtaining a valid consent are vested in the Article 7 and Article 9 (in case special categories of personal data are processed) of the GDPR. In line with that, consent must be freely given, and in order for a data subject to be able to freely assess the possible risks arising from data processing activities to be executed by AI (including exercising the right not to be a subject of an algorithmic decision), data controllers must provide sufficient information to the data subject. Informing obligations of data controllers are laid down in the Articles 12 and 13 of the GDPR with a standard setting referring to the term "average user" which is excluding the personal informational needs.

(4) Strict data protection legislation itself may end up with businesses fearing to develop and implement AI based tools and services. This may, on the other hand, encourage the businesses to find other ways to solve the liability scenarios. Such scenarios must be earlier thought not only in a general risk assessment framework, but also in data protection specific cases.

In the following section, the problems and risks summarized above will be presented via a scenario which will highlight data protection related questions to be tested by the experts. The test aims to find out whether the GDPR already has the answers to those questions, and if yes, whether the answers are consistently accepted by the experts. Another aim of the scenario-based test is to contribute to the current debates by assessing national level expert opinions, as suggested in the EC's White Paper.[20]

2. Hungarian Experts' Opinions

This section reports the Hungarian experts' opinions specific to the regulation of AI technologies from a data protection point of view and within the scope of the problems and risks discussed in the previous section. The method chosen for this work is

[20] White Paper on Artificial Intelligence, 24

the design fiction method which is one of the futures research methodologies[21] that have been practiced both in the industry and academia. Since AI and robots are not yet a usual part of human life, this method could help policy makers to discover the future legal and social implications of specific technologies like AI, even from now. Such an approach is not new, and it has been practiced by the legal academia[22] often and in relation to technology and law. In the present work, scenarios serve as a basis of a standard questionnaire to ensure consistency supported with a standard set of questions referred to the experts before and after they read the scenario. The questions specific to the scenario were testing the expert's overall opinion about the scenario, their opinions on identification of the data controllers, and whether the informing and consent obligations were fulfilled by the data controllers, and if not, how they could have been in a right way. Finally, experts' own case interpretation was asked for in the framework of the inputs given in the scenario.

The experts are chosen based on three criteria which are whether the expert (1) is practicing GDPR either at a law firm or at the Hungarian Data Protection Authority, (2) has a professional interest in AI technologies (published a paper, gave a talk, took part in legal analysis, etc.) and (3) indicated voluntarily be a part of this work. Altogether six Hungarian experts interviewed during the course of the research and their answers will be indicated numerically in the below analysis (specifically, Expert 1, Expert 2, Expert 3, Expert 4, Expert 5 and Expert 6). Seeing how opinions of the experts differ or become closer in interpreting the same case within the same legal framework (GDPR), it helps to improve the interpretation of legal documents for a specific technology. All in all, these qualitative inputs could contribute to the works of either the EU or Hungarian policy makers.

3. The Scenario

In a futuristic scenario where an advanced social robot was purchased by a user, unpredictable outcomes could be reached by processing not only the User's data but the other people entering the User's home and interacting with the Robot. The Robot was initially purchased by the User for assisting in daily home related works such as cooking and cleaning. Once the User suffered from health issues, the Company offered the User some advanced abilities of the Robot, making it possible to support the User's clinical treatment. The Robot was enhanced with the Reinforcement Learning techniques meaning that it could learn via direct interactions from the User. The Robot collected data of the User's daily life, such as important moments in a day together with physiological and psychological data to assess algorithmically how to

[21] Jerome C. Glenn and Theodore J. Gordon, *Futures Research Methodology Version 3.0* (The Millennium Project; 3.0 edition 2009).

[22] Stephanie Ballard and Ryan Calo, 'Taking Futures Seriously: Forecasting as Method in Robotics Law and Policy' (2019) We Robot, University of Miami, School of Law; Christina Mulligan, 'Revenge against Robots' (2018) 69 S. C. L. Rev. 579; Norberto Nuno Gomes de Andrade, 'The application of future-oriented technology analysis (FTA) to law: the cases of legal research, legislative drafting and law enforcement' (2012) 14 Foresight 336, 338.

use them in order to support the User's health. The scenario illustrates the User as an average (consumer) person who does not have any interest in the establishment of an advanced technology and does not pay much time and energy to reading the privacy and consent statements. Once the third party entered into the User's home and interacted with the Robot, data processing of the person became unavoidable through the Robot's algorithmic assessments. The scenario serves questioning the general risks of integrating AI technologies into people's daily lives, as well as the possible data controllership status and responsibilities of the User under the GDPR, and the questions regarding the informing obligations and the consent rules of the Company.

4. General Evaluation of the Scenario and the GDPR Specific Evaluation by the Hungarian Experts

In order to ensure the validity and reliability of the scenario presented, the experts were referred to a question about how they would evaluate the scenario in general. Based on the answers delivered, validity and reliability of the scenario was confirmed by all the experts. They indicated that although the scenario looks futuristic and has many realistic elements pointing out the usefulness of the technologies, the unexpected negative effects from the legal, practical, social, and technological point of views are well-stressed. Hungarian experts are well-aware of the AI technologies and the significance of the challenges it has been raising as they could accurately and even more comprehensively identify all the categories we referred to in the scenario.

A general evaluation of the GDPR specific cases in the scenario was consistently provide by the Hungarian experts. The experts stated that the GPDR is fully applicable to the presented case and that there is no need for amending the GDPR for answering the questions related to AI technologies. No more law is needed since any new piece of law would complicate the implementation more, as they stated, and they believe that the implementation of the GDPR and the future case law would clarify the applicability of the GDPR to AI technologies. However, the Hungarian experts noted the difficulty of accurately identifying the exact rule applicable to a particular case, since the GDPR is not going to be implemented by the national judges in the same way. Especially, the experts pointed to the lack of definitions on AI specific terms such as training data (the input) and the decision (the output) that may cause different approaches among the judges. Furthermore, Expert 5 noted that the GDPR's derogations are quite wide in a way that would result in very different implementation among the national judges. Expert 6 stated that the GDPR only very lately entered into the EU's legislation and without considering certain technologies like AI and block chain, so this could raise some difficulties in the application. Expert 3 referred to the privacy clash between the EU and the US taking different approaches to the right to privacy and to data protection and stated that the GDPR might cause counterproductive results compared to the US where data is treated as a property.

During the interviews, Hungarian experts referred to a variety of legislation to solve the same questions, such as to the long-awaited e-Privacy Regulation, consumer protection law, competition law, civil law, and criminal law. These are clear warning clauses noted by the experts on the uniform applicability of the GDPR rules on AI technologies. Otherwise, the general principles referred to in the GDPR, such as the principle of fairness, accountability, and transparency were found sufficiently applicable to the new technologies like AI (Experts 4 and 5). The most different risk statement was made by Experts 2 and 5, who made a general risk statement with the AI technologies developing out of human control and gaining a level of consciousness which may lead AI to decide on removing the human being from the earth to protect the environment. Although their statements might seem like a piece of sci-fi literature that heavily discusses such risks, the EU policy papers avoided dealing with the question about AI consciousness and human control.

5. Discussion on the Robot User's Role in Operating the Robot

One of the novel questions embedded in the scenario related to the possible responsibilities of the User who is certainly also the data subject. The reasons why this question was related to the degree of control which the Reinforcement Learning technique gives to the User in teaching the Robot directly or assisting it in its learning activities which result in an autonomous decision. Risks arising from the User's instructions changing the AI functionality were also noted in the policy papers presented in Section 1. Since there is no personality defined for robots in law, and there probably will not be in the EU, the purpose of placing this question was to find an alternative answer to the liability scenarios where, in general, the legal persons hold the liability. However, as it is clear and expected from the GDPR's applicability to natural persons in a narrower sense when the question is about their liability, the GDPR's exemptions could be one way to look for possible explanations. Such an exemption is placed in the Article 2 para. 2(c) stating the so-called household exemption that is referring to the data processing activity conducted by a natural person in the course of a purely personal or household activity.

Hungarian experts' answers to the question of possible household exemption on the User's data processing activities, including the question whether the User is a data controller, revealed a variety of approaches. Significantly, most of the experts with law firm affiliation stated that they would try to put the responsibility on the User, while some among them believe that it would not be accepted either by the courts nor by the Hungarian National Supervisory Authority. Expert 1 stated that the case would fall under the household exemption for the User, since the expert compared the use of social media by natural persons similar as the Recital 18 of the GDPR indicates.[23] The Experts 1 and 4's joint opinion pointed the civil liability of the User (as

[23] Recital 18 of the GDPR exempts the natural persons processing personal data in the course of household activity that is not related to a professional or a commercial activity. Social networking, correspondence, and the holding of addresses are given as examples of such an activity. However, the GDPR is still applicable to those

the User puts the input and should be aware of the consequences of the Robot's automated decision-making procedure) to inform the other people interacting with the Robot and take care of its proper functioning. The User shall fulfill informing duties, if not under the GDPR, then under civil law rules, according to the experts. Expert 1 noted that the obligations of the User may not derive from the GDPR, but from the consumer law which puts the responsibility on users to fully understand the product they use. None of the EU policy papers discussed this, therefore this approach is considered to be novel.

Furthermore, whether the User would be identified as a data controller was questioned, and in light of the experts' opinions, it is possible to state that if such a case appears before the Hungarian courts in the future, it will be interpreted in distinctive ways. For example, Experts 2 and 3 stated that the User is a data controller without a doubt, whereas Experts 5 and 6 also defined the User as a data controller and indicated that they would even identify the User as a joint controller. Some Hungarian experts added their own interpretation to the case and extended it in a way that the User would disclose the third party data on a social media account or to a doctor, which then certainly would make the User a data controller. Expert 5 further added that if the User does share the other people's information on a social media account, that would certainly leave the Company out of the responsibility question (with two preconditions, that the Company provides only hardware, and no connection could be made between the software and the User's social media account). When two Hungarian experts working at the Hungarian National Supervisory Authority referred to the same question, they gave opposite answers to each other. While one of the experts said that such a disclosure would not make the User a data controller, the other one opposed to this statement.

On the other hand, Expert 2 did not give any chance for the User to be considered either as a joint controller nor as a data controller by the National Supervisory Authorities or courts, and under any circumstances. The expert was in favor of the full liability of the Company and gave the opinion that the bar for a natural person to be counted as a controller should be very high.

The most different opinion among the experts on the User's liability was delivered by the Expert 6 who made a general evaluation on the applicability of law on non-human beings and stated that it would always be a human who is the main one responsible for any type of technology. Specific to the scenario, the expert noted that both the User and the Company are jointly responsible, but the User bears most of the responsibility since the User is operating and using the Robot, even though the Robot seems like making all the decisions.

named as data controllers or processors providing the means for processing personal data for such personal or household activities. Means of processing is related to "identifying the type of data to be processed, the period for which they would be retained, from which data subjects would the data be collected, who will have access to data, etc." European Data Protection Supervisor, 'Guidelines on the concepts of controller, processor and joint controllership under Regulation' (EU) 2018/1725 1, 9.

6. Responsibilities of the Company

Even though the experts issued different opinions on the applicability of the household exemption to the User, all the experts agreed on the full responsibility of the Company. When the experts were referred to a question about the consent requirements that the Company must fulfill, almost all the experts agreed on the fact that, although consent is not alone enough to perform data processing activities, the Company will surely rely on the consent as a legal basis. The experts stated that the current consent practices shown by the private companies prove that they rely only on consent as a legal basis for their personal data processing activities since it is the easiest to deal with. Expert 2 noted that even if there was no crystal clear legal basis for operating such robots at home in the beginning, it could derive later, but consent should never alone be a legal basis. In the scenario too, the Robot offered such services to the User that were not placed in the purchase contract first, but later the Company chose to request consent for delivering the extra health-care related services. To obtain a valid consent Expert 4 would expect the Company to inform the User and the other people who would interact with the Robot about the risks arising from placing the Robot in a home, but since obviously not included in the GDPR, it would be nonsense to expect it from the Company.

The experts were then referred to a question about how the informing obligation should have been fulfilled by the Company. Besides the general rules visible in the GDPR and the related guidelines, Hungarian experts further noted some particular requirements. For example, Experts 1 and 5 jointly said that the Company should have taken into account the vulnerability of the User and provide the information on this basis. Expert 3, for example, referred to the three methods to be followed by the data controllers for strengthening their valid consent obligation: delivering visual, textual, and oral information which all of them should use at the same time and in accordance with the data subject's personal information needs. About the information specific to the algorithmic decision-making capability of the Robot, Expert 4 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 delivering some of the information to the User. In this case, deciding which information may or may not fall under trade secrets would be the Company's own competence which may cause data subjects to receive incomplete information. This should be, according to the expert, strictly avoided but would require a deep analysis of many different pieces of legislation (e.g. Intellectual Property vs. GDPR).

Finally, the experts were referred to a question regarding the possible data controllers in the scenario which is connected to identifying the person or persons who are to fulfill the consent requirements and informing obligation. Hungarian experts identified the hardware providers (e.g. company delivering the sensors), software provider, data service (e.g. network provider or company providing training data) and database provider in the data controllers network. Manufacturers, developers, engineers, and all users given authorization to access the Robot's services and development phase (even if it is after the purchase) are included in the possible controllership circle which makes identification of the roles and responsibilities complicated.

7. Evaluation and Conclusion

Regulation of AI technologies is one of the hottest debates in the EU policy-makers' agenda. Morevover, with the release of the proposal for regulation of AI technologies, there is much to expect regarding legislation in this sense. The risks specific to the AI technologies have been previously examined in the several research or policy papers prepared for EU institutions, specifically in the studies or papers published by the EP and the EC. According to these papers, technical fundamentals of AI technologies pose a particular risk to the right to data protection, which is regulated under the GDPR. Besides the mass surveillance and profiling in public areas, placing AI-based technologies in households for personal use concretizes the questions related to responsibility and liability. If ML techniques reach such a level that can fully engage users with the training phase of a social robot where they can feed the robot with personal data, and furthermore guide the robot on how to process or use that data, several questions arise on the applicability of the current personal data protection rules. What responsibilities may users have towards the other people interacting with a robot or would they even have any? What are the specific responsibilities of the companies providing AI-based services involving processing of personal data? Would general information they provide to the users be enough to make them fully understand the risks and the right use of the robot?

It is an obvious fact that identifying the data controller(s) during the course of operating a household robot is not an easy task. Based on the technical fundamentals of the AI technologies, even a user who is also a data subject might be assigned a certain level of responsibility for using the technology. While the ultimate responsibility and the liable person obviously will always be the legal persons producing, operating and maintaining robots, their responsibilities and obligations in line with the GDPR remain too general, meaning that specific rules regulating the consent and informing obligation rules must be addressed in the policy options. The GDPR's relevant articles (Arts. 12, 13, 22) do not entail the data controllers providing tailor-made information which needs to be defined conceptually and must be practiced in a way that makes sense. To do that, either at the EU level or at the national level, more guidelines and interpretations are needed, without a doubt. The guidelines should help both data controllers and the data subjects to understand the essence of AI technologies and possible risks arising from use of AI in the framework of a data protection point of view. In order to prevent possible counterproductive results that wrong policy implementations would bring, more scenarios focusing on novel aspects of this novel technology, and expert opinions, including the opinions of the public and civil society, could be obtained helping the policy makers to plan legislation in a better way.