23

"Hey Siri, How Am I Doing?"

Legal Challenges for Artificial Intelligence Alter Egos in Healthcare

Christoph Krönke

I. INTRODUCTION

In response to the question 'Hey Siri, how am I doing?', Apple's intelligent language assistant today only gives ready-made answers ('You're OK. And I'm OK. And this is the best of all possible worlds.'). In the foreseeable future, however, it is quite conceivable that intelligent systems with comprehensive access to the health data of individual users could provide information and assessments of an individual's state of health, make recommendations for a better way of life and possible treatments, and communicate directly with other actors in the medical field (e.g. a treating physician). This opens up the prospect that, with a simple touch of (or even a conversation with) our smartphones, we could enjoy all the promises generally associated with the digitalization of healthcare: comprehensive individual health data would be available and manageable anywhere and anytime, and they could be used to generate high-quality medical diagnoses using Artificial Intelligence (AI), such as those that are already within reach for skin cancer diagnosis[1] or breast cancer detection.[2]

At the same time, the perspective on AI Alter Egos in the health sector raises numerous legal questions. The most essential of these increasingly pressing issues shall be identified and briefly discussed in this contribution – in a way that is understandable not only for die-hard lawyers.[3] First and foremost, responsible AI Alter Egos in healthcare would certainly require, on the one hand, a high level of data protection and IT security, for example, with regard to an individual's informed consent to the data processing and with respect to the (centralized or decentralized) storage of health data. On the other hand, such dynamic systems would pose particular challenges to medical devices law, for instance with regard to the necessary monitoring of a self-learning system with medical device functions. Furthermore, conflicts of interest between the areas of law involved are becoming apparent, particularly with regard to the rather restrictive, limiting approach of data protection law on one side of the spectrum, and the rules of product safety law aiming for efficiency, high quality, and high performance of applications on the other

[1] There are already analytical methods for the detection of skin cancer that can be implemented using a commercially available smartphone and that are significantly more powerful than the cognitive abilities of the average dermatologist, cf. A Esteva and others, 'Dermatologist-Level Classification of Skin Cancer with Deep Neural Network' (2017) 542 *Nature* 115, 117 *et seq*.

[2] See e.g. ED Pisano, 'AI Shows Promise for Breast Cancer Screening' (2020) 577 *Nature* 35, 35 *et seq*.

[3] Many of the legal considerations I am making in this chapter are essentially based on my thoughts on data protection and medical devices law developed in my habilitation thesis, published as C Krönke, *Öffentliches Digitalwirtschaftsrecht* (2020) 467 *et seq*. (data protection law) and 500 *et seq*. (medical devices law).

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

side. With my considerations I would like to show that, all in all, the development of AI Alter Egos in healthcare will require an evolving interpretation of the applicable legal frameworks while – at the same time – ensuring that these systems make responsible decisions. Ignoring either of these necessities would put both the individual patient's (data) sovereignty and the quality of the system outputs at stake.

I would like to proceed as follows: first of all, I would like to outline and describe the functionalities of AI Alter Egos in the healthcare sector,[4] namely the functions of an Alter Ego as a program for storing and managing individual health data,[5] as a software for generating individual medical diagnoses,[6] and finally as an interface for a collective analysis and evaluation of Big Health Data.[7] On this basis, I will identify the key elements of the applicable legal framework and discuss the three basic functions of an AI Alter Ego in light of the basic requirements following from this framework.[8] In doing so, I will focus primarily on the supranational requirements of European Union law so as not to become entangled in the thicket of national legislation.[9]

II. AI ALTER EGOS IN HEALTHCARE: CONCEPTS AND FUNCTIONS

In determining the concept and the description of the aforementioned functions of an AI Alter Ego in the healthcare sector, I am guided primarily by the considerations of *Eugen Münch*[10] who has been developing the idea of a digital Alter Ego for decades[11]. This is mainly due to the fact that his ideas seem very sound and general and do not reflect a concrete business model, but rather the main features that any AI Alter Ego in healthcare could have. Moreover, *Münch* had anticipated much of what many digital assistants and smart objects are designed for today. In the context of this contribution, it should remain open whether the carrier of an Alter Ego in the healthcare sector should be one or more decidedly state players or (public or private) economic enterprises, and whether the Alter Ego can operate on the basis of a specific legal framework or on the general basis of private contracts.[12] Certainly, the past has shown that the innovative and performance capabilities of private sector players are often superior to those of digital government initiatives. Even if Alter Ego projects should initially come from the private sector, however, one thing must be clear from the outset: the overriding (ethical) principle behind the idea of an Alter Ego in the health sector is not to enable utmost economic usability of health data, but rather to preserve the data sovereignty of the individual.

[4] See Section II.

[5] See Section II 1.

[6] See Section II 2.

[7] See Section II 3.

[8] See Section III.

[9] For this reason, specific national legislation, such as the provisions of the 2019 Digital Supply Act (*Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation)* (Digitale-Versorgung-Gesetz, DVG) will not be covered. For more information on this legislation cf. J Kühling and R Schildbach, 'Die Reform der Datentransparenzvorschriften im SGB V' (2020) 2 *NZS* 41, 41 *et seq*.

[10] Founder of the *Münch Foundation*. See www.stiftung-muench.org/.

[11] See e.g. the report on *Eugen Münch*'s idea: A Seith 'Sanierung via Laptopmedizin' *Der Spiegel* (12 January 2005) www.spiegel.de/wirtschaft/landklinik-sterben-sanierung-via-laptopmedizin-a-387338.html. *Münch* recently appointed an informal 'Digital Alter Ego' expert commission, of which I have been a member since early 2020.

[12] These are highly significant *organizational* issues that are undoubtedly crucial to the success of any Alter Ego project. However, they depend on the political will and the specific legal framework of individual countries and therefore cannot be discussed in detail in this chapter.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

This being said, the general idea of an AI Alter Ego in healthcare involves two components and key functions: database functions and diagnostic functions.

1. *Individual Health Data Storage and Management*

The prerequisite for AI Alter Egos is a vast database that contains and manages as much personal health data of individual users as possible. In the ideal case, the entire individual data stock forms and reflects a digital image of the physical condition of the individual – in other words, a (complete) digital 'Alter Ego'. In this way, the individual user has (at least theoretically) full access to the health-related information relating to him or her and can grant third parties, such as physicians, health companies, or insurances, access to a specific or several data areas too; subject, of course, to the practically, highly critical question of suitable data formats and interfaces. From a purely technical point of view, storage of the health data of all Alter Egos in a central database is just as conceivable as decentralized storage on systems that are controlled by the individual users or trustworthy third parties. However, as has been stated at the outset, the Alter Ego is designed as a tool that is intended to serve, first and foremost, as a benefit to the user. It shall, therefore, enable him or her to decide independently and responsibly ('sovereignly') on the access to and use of his or her health data. This idea of the individual's health-specific 'data sovereignty' can hardly be reconciled with a central storage of his or her data – let alone with an outsourcing in 'health clouds' located beyond European sovereign borders.

2. *Individual Medical Diagnostics*

Building on this storage and management function, the digital Alter Ego should also have the potential to generate customized and high-quality medical diagnoses, taking into account all available health-related data points of the individual, possibly monitored on a real-time basis. When classifying this second, diagnostic function, however, one should follow a strict sense of reality. On the basis of the common differentiation, to be thought of on a sliding scale, between 'weak' (or 'narrow') AI, which is merely involved in the processing of concrete, relatively limited tasks, and 'strong' (or 'general') AI, which can be entrusted with comparatively comprehensive tasks like a human doctor,[13] all of the intelligent diagnostic systems that are, will, or might be implemented in the foreseeable future can be clearly classified as forms of narrow AI, with very specific functions such as cloud-based applications that analyze and interpret computed tomography (CT) images using self-learning algorithms to prepare medical reports[14]. Strong intelligent systems, on the other hand, are the stuff for science fiction novels and movies and should therefore not be the basis for legal considerations.

[13] Cf. for this differentiation for instance I Revolidis and A Dahi 'The Peculiar Case of the Mushroom Picking Robot: Extra-contractual Liability in Robotics' in M Corrales, M Fenwick, and N Forgó (eds), *Robotics, AI and the Future of Law* (2018), 57–59; see also the differentiation made in the AI strategy of the German Federal Government: Die Bundesregierung, 'Strategie Künstliche Intelligenz der Bundesregierung' (KI Strategie Deutschland, November 2018) 4, 5 https://www.bmbf.de/bmbf/shareddocs/downloads/files/nationale_ki-strategie.pdf?__blob=publicationFile&v=1.

[14] In 2019, for example, the Siemens AI-based AI-Rad Companion Chest CT program was the first application of the company's AI-Rad Companion platform to receive CE marking (see M Bludszuweit, 'KI-basierte Software AI-Rad Companion Chest CT von Siemens Healthineers für Europa zugelassen' (Siemens Healthineers, 26 July 2019) www.siemens-healthineers.com/de/press-room/press-releases/pr-20190726028shs.html). The program evaluates CT images of the thorax from any source, highlights abnormalities with respect to the corresponding organs (heart or lung), the carotid artery and vertebrae, and automatically generates a report for the radiologist, including any indications of possible abnormalities.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

3. *Interface for Collective Analysis and Evaluation of Big Health Data*

The performance of the diagnostic functions depends on the quantity and quality of the health data, on the basis of which the algorithms used in the Alter Ego are trained and ultimately formed into robust decision rules. Against this background, a possible third, rather secondary function of the digital Alter Egos in their entirety could be to provide an all-encompassing data basis for its various possible diagnostic functions. In this respect, the individual Alter Ego could be both the limiting and enabling interface for a supra-individual (collective) analysis and evaluation of Big Health Data, from which the individual 'data sovereign' could ultimately benefit. Even if this function is reminiscent of the dystopian scenario in which humans merely act as data sources and mutate into 'transparent patients' – the price of any medical evaluation method, however advanced, is always the availability of a comprehensive basis of health data.

III. KEY ELEMENTS OF THE LEGAL FRAMEWORK AND LEGAL CHALLENGES

As explained in the introduction, the legal framework for the establishment and operation of digital Alter Egos is primarily provided by European data protection law[15] and the law on medical devices.[16] In the following, I will put each of the aforementioned functions of an Alter Ego against the background of these legal rules and assess the prospect of AI Alter Egos in healthcare under the existing legal framework. In doing so I will focus on the scope of application as well as the material goals and basic concepts of these regimes.

1. *European Data Protection Law*

In order to adequately assess the specific data protection standards in their relevance for Alter Egos, it is not sufficient to make general references to the protection of informational self-determination or the rights to privacy and the protection of personal data.[17] As a matter conceived in terms of 'risk law',[18] data protection law shields the rights and interests of the persons concerned from various risks that can be typified to a certain extent. The resulting need for protection forms the actual concrete purposes of data protection law. The processing of personal data by digital Alter Egos touches on several of these purposes, which, in turn, can be assigned to the two fundamental protection concepts of data protection law, namely, the limitation and transparency of data processing.[19] Taking account of the different basic functions of AI Alter Egos, the following major data protection goals can be distinguished in the context of AI Alter Egos in healthcare.

[15] See Section III 1.

[16] See Section III 2. The applicable Medical Devices Regulation will be supplemented in the foreseeable future by the EU Artificial Intelligence Act, which at least in its draft version (see COM(2021) 206 final) refers to the Medical Devices Regulation and modifies it slightly with regard to high-risk systems.

[17] See the Charter of Fundamental Rights of the European Union (26 October 2012) 2012/C 326/02 (Charter of Fundamental Rights), Articles 7 and 8.

[18] The characterization of data protection law as a risk-focused legal regime seems not to be controversial, even though it is rarely explicitly addressed – see as an exception for example K Ladeur, 'Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?' (2009) 62 *DÖV* 45, 53 et seq.

[19] Cf. with reference to the distinction of (limiting) opacity tools and (transparency-creating) transparency tools by P De Hert S Gutwirth 'Regulating Profiling in a Democratic Constitutional State' in E Claes, S Gutwirth, and A Duff (eds), *Privacy and the Criminal Law* (2006) 67 *et seq.*; N Marsch, *Das europäische Datenschutzgrundrecht* (2018) 96 *et seq.*, who refers to these concepts as 'protection goals'.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

a. Limitation of Data Processing: Data Protection-Friendly and Secure Design

The individual data storage and management functions of Alter Egos easily activate the data protection requirements under both the General Data Protection Regulation (GDPR)[20] and the supplementary European basic rights on data protection.[21] All health-related information relating to individuals is personal data – even particularly sensitive in the sense of Article 9 of the GDPR – and all possible 'work steps' of data handling by the Alter Ego are subject to the processing operations defined in Article 4(2) of the GDPR, such as the collection, storage, reading, querying, matching, use, modification, and transmission of personal data.

Additionally, with regard to the function of Alter Egos as interfaces to a collective database for a comprehensive analysis and evaluation of Big Health Data, the data protection rules are likely fully applicable as well. In the context of medical treatments, almost every piece of information can be assigned a personal and health reference that makes the person behind it at least 'identifiable' in the sense of Article 4(1) GDPR. In particular, medical data like a large blood count or an ECG recording are so unique to an individual that they can hardly be fully anonymized. Complete technical anonymization, which would lead to the inapplicability of data protection law, is therefore illusory. In this respect, it is certainly true that, in principle, 'anonymous data' no longer exists in the healthcare sector.[22]

The data protection rules of the GDPR will thus subject almost every single processing of health-related data in Alter Egos to certain requirements with regard to the 'whether' and 'how' of data processing. With regard to the 'whether' of lawful data processing, Article 6(1) GDPR establishes the principle that processing of personal data is only permissible if it can be based on one of the processing situations mentioned in Article 6(1)(a) to (f) GDPR (the so-called prohibition principle). In particular, Articles 6(1)(a) and 9(2)(a) as well as Articles 6(1)(e) and 9(2)(g) and (h) of the GDPR can be considered as the predominant legal basis for the processing of health data by an Alter Ego, since the processing operations would be regularly based either on the explicit consent of the users or on specific legal provisions introduced by Member States in order to create a legal basis for the storage, management, and diagnostic analysis of individual health data. In addition, the opening clause of Article 9(2)(j) GDPR may also become relevant specifically for collective analysis and evaluation. This allows Member States to create legal processing powers for 'scientific research purposes' to a large extent, including also private research.[23] This legitimizes researchers to process health data even without the consent of the data subjects. Despite all the emphasis on the high level of protection in the health sector, the GDPR thus gives research interests comprehensive priority over the data protection interests of the data subjects.

[20] 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), OJ 2016 L 119/1.

[21] See in particular Articles 7 and 8 of the Charter of Fundamental Rights.

[22] Cf. M Martini and M Hohmann 'Der gläserne Patient: Dystopie oder Zukunftsrealität? Perspektiven datengetriebener Gesundheitsforschung unter der DS-GVO und dem Digitale-Versorgung-Gesetz' (2020) 49 *NJW* 3573, 3574 (hereafter Martini and Hohmann, 'Der gläserne Patient'). Due to this lack of watertight anonymization possibilities *de facto*, they plead for the introduction of a concept of *legal* anonymization *de lege ferenda*, which would eliminate the identifiability of a data subject through health data by legal fiction, as long as sufficient technical and organizational security measures were in place.

[23] It should be noted that this (wide) interpretation of the term 'research' is disputed in legal scholarship. Some authors would like to interpret Art. 9 GDPR as exclusively referring to research in the public interest, see e.g. T Weichert 'Art 9 Verarbeitung besonderer Kategorien personenbezogenere Daten' in J Kühling and B Buchner (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (2nd ed. 2018) para 122. For a view similar to the one taken in this contribution cf. for instance, Martini and Hohmann, 'Der gläserne Patient' (n 22) 3576.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

With regard to the 'how' of lawful data processing, Article 5 GDPR defines the essential 'principles of data processing', which include in particular the principles of purpose limitation,[24] data minimization[25] and storage limitation[26]. In addition to these basic processing rules, the Union's data protection legislation contains numerous other provisions. Some of these supplement the basic rules with sector-specific requirements, for example, with the particularly strict requirements for the processing of health-related data pursuant to Article 9 GDPR. Others specify, concretize, and flank them in more detail, for example in the rights of data subjects pursuant to Article 12 et seq. GDPR, and in some cases they do so by adding structural requirements beyond concrete data processing, like by requiring data protection-friendly and secure technology design in accordance with Article 25(2) and Article 32 GDPR.

In more concrete terms, the principle of purpose specification and limitation under Article 5 (1)(b) GDPR requires that the information be collected only 'for specified, explicit and legitimate purposes' and 'not further processed in a way incompatible with those purposes'. The importance of this principle is underlined by its embodiment in Sentence 1 of Article 8(2) of the Charter of Fundamental Rights. Therefore, the storage of health and other personal data 'for undetermined and not yet determinable purposes' is clearly impermissible under European Union law.[27] Otherwise, the data subjects would no longer be able to see by which bodies the specifically collected personal data are processed in which context. The principle of purpose limitation is supplemented by the principles of data minimization and necessity under Article 5 (1)(c) GDPR. Accordingly, the collection and storage of each piece of information must be necessary in relation to the specified processing purposes, in other words, it must be necessary for the specified diagnostic and other medical purposes. In the case of health-related information of a particularly sensitive nature, the need for data collection may be condensed into a specific decision to be taken.

Against this background, any storage of health data would have to be carried out for a definable medical purpose from the outset. The monitoring of bodily functions 'into the blue', that is, for yet unknown medical purposes that might (or might not) become relevant in the future, seems inadmissible. The creation of a 'digital Alter Ego' in the sense of a complete image of all physical processes in the patient's body, irrespective of an existing medical need, is therefore hardly possible under current data protection law – at least at first glance.

The specific requirements that can be derived from the principle of purpose limitation and the principle of necessity and data minimization continue to apply when accessing and retrieving information stored in the Alter Ego. For example, the principle of purpose limitation prohibits the processing of stored data for purposes that are not compatible with the originally defined purpose of collection. Accordingly, changes of purpose with regard to the processing of health-related data are only permissible if the conditions set out in Article 6(4) GDPR are met. Thus, either the (explicit) consent of the data subject is obtained[28] or another reason pursuant to Article 9(2) GDPR is available, in which case an additional compatibility check is to be carried out in accordance with Article 6(4) GDPR additionally.[29]

[24] Article 5(1)(b).

[25] Article 5(1)(c).

[26] Article 5(1)(d).

[27] Cf. (in a different, public context) CJEU, Joined Cases C-293/12 and C-594/1 *Digital Rights Ireland Ltd v Minister for Communications and Others* (8 April 2014).

[28] See GDPR, Article 9(2)(a).

[29] For a detailed analysis of the requirements following from GDPR, Article 6(4) see e.g. B Buchner and T Petri 'Art 6 Raeumlicher Anwendungsbereich' in J Kühling and B Buchner (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (3rd ed. 2020) paras 178 *et seq*.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

Such changes of purpose will likely become inevitable with the increasing use of Alter Egos as well as the extension of their diagnostic function. One could think of information initially collected and stored solely for the purpose of monitoring cardiovascular functions that is later being processed for the purpose of cancer detection, too. As long as the general medical purpose of data processing is not abandoned, the compatibility test for both individual diagnostic and collective analysis and evaluation purposes is in general complied with; provided an interpretation taking the individual's interest in the performance of his or her own Alter Ego into account is carried out. However, this performance depends crucially on the fact that health data which were initially collected in a permissible manner can also be processed for additional purposes, including the generation of decision rules on the basis of large supra-individual (big data) databases. With regard to general research purposes, this idea has been explicitly laid down in the GDPR: according to Article 5(1)(b) GDPR, processing for (further) scientific research purposes is 'not considered incompatible with the original purposes'. This flexibilization of the purpose limitation principle does not exempt the person responsible from checking the compatibility of the secondary purpose with the primary purpose according to Article 6(4) GDPR on a case-by-case basis, the principle of purpose limitation is still valid – as a rule, however, he may assume that compatibility is guaranteed.[30]

Most certainly, the conception of a comprehensive individual health database, which can also form the foundation for potential collective (Big Health) data analysis and evaluation processing, involves highest structural dangers and risks with respect to both the lawfulness of the processing and the security of the stored information.[31] Automated processing of health data and the accessing of these data (both on the basis of centralized and decentralized storage system) entail a particular risk of inadmissible or even abusive input and accessing. This is in obvious tension with the requirements in Articles 24 and 25(1) GDPR, according to which the responsible body must take 'appropriate technical and organisational measures', taking into account the relevant risks, which serve to 'implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary guarantees in the processing in order to meet the requirements of this Regulation and protect the rights of the data subjects'. Similar structural requirements are laid down in Article 32 GDPR specifically with regard to data security.[32]

[30] Cf. A Roßnagel, 'Datenschutz in der Forschung' (2019) 4 *ZD* 157, 162.

[31] It should be mentioned that the field of 'data protection and Big Data' has become a subject of extensive research and will, as such, not be further discussed here. See e.g. T Weichert 'Big Data und Datenschutz – Chancen und Risiken einer neuen Form der Datenanalyse' (2013) 6 *ZD* 251; A Roßnagel, 'Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht'(2013) 11 *ZD* 562, 562 *et seq*.; JP Ohrtmann and S Schwiering, 'Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze' (2014) 41 *NJW* 2984, 2984 *et seq*.; T Helbling, 'Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung' (2015) 3 *K&R* 145, 145 et seq.; P Richter, 'Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO' (2015) 39 *DuD* 735, 735 *et seq*.; C Werkmeister and E Brandt, 'Datenschutzrechtliche Herausforderungen für Big Data' (2016) 4 *CR* 233, 237 *et seq*.; K Ladeur, '"Big Data" im Gesundheitsrecht – Ende der Datensparsamkeit?"' (2016) 40 *DuD* 360, 360–361; N Culik and C Döpke, 'Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data Anwendungen – Analyse möglicher Auswirkungen der DS-GVO' (2017) 5 *ZD* 226, 228; T Hoeren, 'IT- und Internetrecht – kein Neuland für die NJW' (2017) 22 *NJW* 1587, 1591; BP Paal and M Hennemann, 'Wettbewerbs- und daten(schutz) rechtliche Herausforderungen' (2017) 24 *NJW* 1697, 1700 *et seq*.; see also the contributions of G Hornung, 'Erosion traditioneller Prinizpien des Datenschutzrechts durch Big Data' and Y Hermstrüwer, 'Die Regulierung der prädikativen Analytik: eine juristisch-verhaltenswissenschaftliche Skizze' in W Hoffmann-Riem (ed), *Big Data – Regulative Challenges* (2018) 79, 99.

[32] The relationship between GDPR, Article 32 and Article 24 *et seq*. DSGVO is illuminated by M Martini in BP Paal and DA Pauly (eds), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO/BDSG* (2nd ed. 2018) paras 7 *et seq*.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

In view of the obligations to ensure that technology is designed in a 'privacy by design' manner, it is imperative for any healthcare Alter Ego system that a highly effective access rights management system be introduced that is absolutely subordinate to the 'health data sovereignty' of the individual. Furthermore, in view of the high risks involved, it is likely to be imperative to develop a decentralized (rather than a centralized) data storage system. Against this background, the ethical principle of data sovereignty of the individual also forms a legal principle with binding organizational effects for any Alter Ego in healthcare.

b. Securing a Self-Determined Lifestyle and Protection from Processing-Specific Errors through Transparency

In contrast to its database functions, the diagnostic function of an AI Alter Ego rather faces the typical data protection objectives that apply to all intelligent AI systems. Especially, the specific lack of transparency of algorithmically controlled decisions of intelligent systems challenges the goal of guaranteeing an autonomous self-determined lifestyle. An example with special relevance to data protection law is medical diagnoses that are made according to rules based on Big Data procedures. These decisions are typically based firstly on correlations (and thus not necessarily on causalities) and secondly on a multitude of different health-related data in the context of the concrete decisions. The results of the medical recommendations of an Alter Ego in the healthcare sector could range from the (comparatively harmless) recommendation to take a walk to stimulate the circulation to more sensitive predictions such as suspected sugar disease or a skin cancer diagnosis. If the rules and factors relevant to the decision in question, particularly with regard to the relevance of certain health-related and other personal circumstances, are not sufficiently clear to the person affected by the decision, this person has, on the one hand, no opportunity to adjust his or her behavior to the decision and, on the other hand, cannot recognize or correct factual errors of the Alter Ego.[33] In such a context, an autonomous, self-determined way of life appears to be possible only to a limited extent as the range of diagnostic possibilities increases. For such reasons, the creation of transparency in data processing has long been a recognized principle of data protection law.[34] The diagnostic function of an Alter Ego operating by means of AI is, therefore, in a specific tension between this principle and the many transparency-securing provisions of data protection law.

Furthermore, the use of intelligent systems such as AI Alter Egos in healthcare regularly touches on the need to protect the data subject from processing operations based on inappropriate decision rules. For example, if the decisions fail to achieve their medical (data processing) purpose due to inappropriate programming or use of the Alter Ego, they might generate inappropriate output. On the one hand, this addresses the possible specific quality problems of intelligent systems in general.[35] These problems can be based on various factors, such as the inferiority of the data basis used for the development of the decision rules, the improper or even illegal programming of the Alter Ego, or its use in a context that is not suitable for it. On the other hand, a specific element of the regulatory objective of avoiding inappropriate output of data processing lies in the protection against discrimination specific to data processing. What is meant is not unequal treatment as such, which occurs when a person is discriminated against based on particularly sensitive personality traits such as origin or disability. Rather, it refers to

[33] Cf. M Martini, *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz* (2019) 30 *et seq*.

[34] See GDPR, Article 5(1).

[35] Cf. for example T Wischmeyer, 'Regulierung intelligenter Systeme' (2018) 143 *AöR* 1, 23 *et seq*. who also treats quality control as an overarching regulatory concern and protection against discrimination as a special problem of 'failure' of intelligent systems.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

more disadvantageous treatment in a broader sense; this is when the person concerned belongs to a group of persons previously formed by the system. This second definition includes circumstances in which persons are assigned to a group that was defined specifically for one person by the system in the first place. Therefore, such groups can be understood as 'tailor-made'.

The decision-making rules of an Alter Ego in the health sector will typically be based on the linking of certain health or other personal data points, like name, place of residence, educational level or income, eating, and other habits. These data points are often 'developed' by the system itself and typically include the results expected from the output of the Alter Ego, such as a specific diagnosis of a disease or general life expectancy. Even though Big Data procedures in particular aim to achieve the most granular classifications and evaluations by including as many data points as possible, these procedures inevitably lead to the formation of groups of people and a certain expectation or evaluation. To provide an example: higher risk of suffering from a certain disease might be linked to the affiliation to a certain group profile, for instance, people with a foreign name, a place of residence with low purchasing power, an unhealthy diet, moderate exercise, no university studies, etc. Because the Alter Ego does not necessarily include all individual health-related characteristics of a person and rather decides merely on random group membership based on more or less health-related (and other personal) data, a negative decision for the person with the desired characteristic (like low risk of illness) contrary to the system expectation based on his or her profile may prove to be arbitrary.[36]

One aspect however must be particularly emphasized at this point, as it is often not sufficiently taken into account in legal scholarship:[37] data protection law itself does not prohibit incorrect or unlawful outputs, and in particular it does not prohibit general discrimination. The fact that unequal treatment based on gender, origin, other group memberships, or simply arbitrariness is not permissible does not follow from data protection regimes, but rather from substantive anti-discrimination legislation. Only the *structural bias* of automated data processing in general and of intelligent Alter Egos in particular is relevant from a perspective of data protection law. Such structural biases include the tendency to treat individuals in relation to a specific (medical) processing purpose on the basis of selective, typifying characteristics and this treatment being potentially inappropriate, arbitrary, and/or contrary to the purpose of the processing.

2. *European Medical Devices Regulation*

In the healthcare sector, such substantial-qualitative normative requirements – which cannot be derived from data protection law itself – arise from European medical devices law with regard to the outputs of an AI Alter Ego. According to the two introductory recitals of the applicable Medical Devices Regulation (MDR),[38] European medical devices law not only aims to ensure a functioning internal market for medical devices and thus pursues both cross-border coordination and economic promotion purposes, it is also supposed to guarantee high standards with regard to the quality (performance of the products) and safety (prevention of hazards and risks) of medical devices. First of all, it depends on the medical device legal classification of the individual

[36] Cf. with regard to AI-based decisions in general M Martini, *Blackbox Algorithmus* (n 33) 50.

[37] See for the following considerations C Krönke, *Öffentliches Digitalwirtschaftsrecht* (2020) 500 *et seq.*

[38] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ 2017 L 117 (MDR).

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

functions of an AI Alter Ego[39] whether and to what extent the general objectives and the specific requirements of MDR[40] apply.

a. Classifying AI Alter Ego Functions in Terms of the Medical Devices Regulation

It goes without saying that software like an AI Alter Ego or, more precisely, individual functions of it can be classified as 'medical devices' in the legal sense. Software and software-supported products have been playing a significant role in the markets for medical services in the broader sense for some time. Possible distribution channels include software purchase or software rental as well as purely remote sales-based diagnostic or therapeutic services.[41] Possible applications which could also be used as part of an Alter Ego system range from comparatively simple computer programs, such as classical practice software for maintaining electronic patient records or health-related smart watch functions[42], to more complex, intelligent programs and systems, such as cloud-based applications that analyze and interpret computed tomography (CT) images using self-learning algorithms to prepare medical reports.[43] A differentiation between different types of applications is particularly useful with regard to the respective use context intended, as the distinction between medical devices and non-medical devices as well as the classification according to different risk classes[44] is primarily based on the intended purpose of the product.[45] Against this background, four types of software functions can be distinguished from the outset in the context of AI Alter Egos in healthcare: (1) functions that qualify as 'software as a medical device' (so-called stand-alone software or software as a medical device – SaMD) and as (2) software as an accessory of a medical device; furthermore, Alter Ego functions that fall within the category of a (3) software as a component of a medical device (so-called integrated software), and finally (4) functions that merely qualify as software in the medical field.[46]

First of all, (1) certain Alter Ego functions could fall under the term 'medical devices' in themselves, if they are intended to fulfil one of the 'specific medical purposes' mentioned in Article 2(1) MDR, i.e. if they are intended to diagnose, monitor or treat diseases, injuries or disabilities. A direct effect in or on the human body is not necessary for this purpose; a provision 'for human beings' is sufficient, even if it is only aimed at indirect physical effect.[47] In this sense

[39] See Section III 2(a).

[40] See Section III 2(b).

[41] Such sales forms are also explicitly covered by medical devices law, see MDR, Article 6.

[42] For functions of the Apple Watch (so far in versions 4 and 5) there are CE markings for an 'ECG App', which records a 1-channel electrocardiogram (ECG) and evaluates it with regard to atrial fibrillation (AFib), as well as a function 'Messages in case of irregular heart rhythm', which analyses the pulse rate with regard to irregularities indicating AFib (see the description on www.apple.com/de/healthcare/apple-watch/).

[43] See the references earlier at (n 14).

[44] See MDR, Annex VIII 3(1): 'The application of the classification rules depends on the intended purpose of the products'.

[45] See the legal definition in Article 2(1) MDR, according to which each medical device 'shall fulfil one or more of the specific medical purposes [described in detail in the regulation]'.

[46] Cf. on this common classification, which is also the basis for the scheme of the Commission's Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, European Commission DG Internal Market, Industry, Entrepreneurship and SMEs, 'Medical Devices: Guidance document' (2016) *MEDDEV* 2.1/6 9 *et seq*. (hereafter European Commission, 'Medical Devices'), for example R Oen, 'Software als Medizinprodukt' (2009) 2 *MPR* 55, 55 *et seq*.; M Klümper and E Vollebregt, 'Die geänderten Anforderungen für die CE-Kennzeichnung und Konformitätsbewertung auf Grund der Richtlinie 2007/47/EG' (2009) 2 *MPJ* 99, 100-101; S Jabri, 'Artificial Intelligence and Healthcare: Products and Procedures' in T Rademacher and T Wischmeyer (eds), *Regulating Artificial Intelligence* (2020) 307, 314 *et seq*.

[47] CJEU, C-329/16 *Snitem and Philips France* (26 January 2018) paras 27 *et seq* (herafter *Snitem and Philips France*).

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

(and explicitly according to the former directive terminology) 'independent'[48] software products are considered 'active' medical devices under Article (4) MDR, for which specific classification rules and material requirements apply; they are also subject to special regulations, such as those of the MDR's UDI[49] system). Practical examples of such SaMDs are decision-support programs comparing medical databases with the data of individual patients in order to provide medical personnel or patients directly with recommendations for the diagnosis, monitoring, or treatment of the patient in question.[50] The complex systems for the (possibly adaptive) analysis of image and other data with descriptive, predictive, or prescriptive functions mentioned earlier in this contribution also fall into this group of software products. This category is probably the most relevant for the diagnostic functions of an AI Alter Ego in healthcare.

Other Alter Ego functions will qualify as (2) 'accessories' in the sense of Article 2(2) MDR.[51] In contrast to (completely independent) standalone software, accessory software does not fulfil a specific medical purpose itself. However, it does fulfil such a purpose in combination with one or more other 'medical devices', by enabling or at least supporting its specific function as a medical device. In particular, software marketed separately for programming and controlling medical devices as well as their integrated software (e.g. of pacemakers)[52] is regularly qualified as accessory software. Against this background, support software that is compatible with an AI Alter Ego but marketed separately could fall within the category of an accessory.

Distinct from these first two categories are (3) supportive Alter Ego functions forming an integral part of one or more other Alter Ego functions that qualify as medical devices at the time of the placing on the market.[53] Important examples of such integrated software include programs for the control of medical devices, like blood pressure monitors[54] or the power supply.[55] Such programs are not treated as medical devices themselves but as mere components of the respective product.

In contrast, (4) all other functions of an AI Alter Ego would have – as such! – no relevance under medical devices law. These can be programs with essential but merely auxiliary functions such as collecting, archiving, compressing, searching, or transmitting data. Examples include important information and communication systems that are connected with the diagnostic functions of the Alter Ego such as communication systems for separate tele-medicine services,[56]

[48] Cf. critically with regard to the renouncement of this terminology in the MDR and the practical consequences of this renouncement UM Gassner, 'Software als Medizinprodukt – zwischen Regulierung und Selbstregulierung' (2016) 4 *MPR* 109, 110–111. The previous differentiation between independent and integrated software therefore should remain valid.

[49] Short for Unqiue Device Identification.

[50] See German Federal Office for Drugs and Medical Devices, 'Orientierungshilfe Medical Apps' (*BfArM*, 1 November 2015) https://docplayer.org/63901775-Bfarm-orientierungshilfe-medical-apps.html point 3 (hereafter BfArM, 'Orientierungshilfe Medical Apps'). Such a program was also the subject of the proceedings in CJEU, *Snitem and Philips France* (n 47) paras 17 *et seq*. After entering individual patient data, the program alerted the user to possible contraindications, interactions with other drugs and overdoses, etc.

[51] From recital 19 sentence 2 of the MDR it becomes clear that software can actually be accessories. This was previously controversial, see UM Gassner, 'Software als Medizinprodukt – zwischen Regulierung und Selbstregulierung' (2016) 4 *MPR* 109, 111.

[52] Cf. for this example M Klümper and E Vollebregt, 'Die geänderten Anforderungen für die CE-Kennzeichnung und Konformitätsbewertung auf Grund der Richtlinie 2007/47/EG' (2009) 2 *MPJ* 99, 100.

[53] Cf. for a general definition of 'integrated' medical software e.g. R Tomasini, *Standalone-Software als Medizinprodukt* (2015) 44.

[54] Cf. for this example G Sachs, 'Software in Systemen und Behandlungseinheiten' in UM Gassner (ed), *Software als Medizinprodukt – IT vs. Medizintechnik?* (2013) 31 *et seq*.

[55] M Klümper and E Vollebregt, 'Die geänderten Anforderungen für die CE-Kennzeichnung und Konformitätsbewertung auf Grund der Richtlinie 2007/47/EG' (2009) 2 *MPJ* 99, 100.

[56] Cf. BfArM, 'Orientierungshilfe Medical Apps' (n 46) point 3.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

medical knowledge databases,[57] hospital information systems (HIS) with pure data collection, administration, scheduling, and accounting functions as well as picture archiving and communication systems (PACS) without reporting function[58]. Furthermore, as recital 19 sentence 1 of the MDR states in principle, programs used for lifestyle and well-being purposes are not sufficiently related to specific medical purposes. These include, in particular, the functions of a Smartwatch for recording and evaluating movement calories or sleep rhythm when using a lifestyle app. Of course, software with completely unspecific functions, for example operating systems or word processing program, are also irrelevant under medical devices law. Against the background of these considerations, software serving the individual data storage and management function of an AI Alter Ego as well as possible functions aiming for the collective analysis and evaluation of the (big) health data gathered through the participating Alter Egos in their entirety would – as such! – not qualify as 'medical devices' or 'accessories' under the MDR.

This does not mean, however, that the individual database functions and the collective Big Health Data functions of an AI Alter Ego are entirely irrelevant under medical devices law. It is not only the diagnostic functions being relevant. Of course, the usual case in practice[59] deals with information technology systems consisting of several modules. In such instances, some of these modules can be qualified typically as a medical device or accessory, while other modules can only be qualified as software in the medical field. Consequently, the rules of medical devices law, especially the obligation to label, only apply to the first-mentioned modules.[60] Nevertheless, it has probably become clear that the performance of the diagnostic functions of an AI Alter Ego is crucially dependent on the quantity and quality of the data sets, including the software used to store and manage, analyze, and evaluate them. Even if the databases and their management software as well as the algorithms used to analyze and evaluate them are not subject to medical devices law as such, their quality and design has a decisive influence on how the diagnostic functions are to be assessed under medical devices law. In this respect, the individual database functions and the Big Health Data functions of an AI Alter Ego are not directly, but indirectly relevant for the following medical devices law considerations.

b. Objectives and Requirements Stipulated in the MDR

The potentially high quantitative and qualitative performance of the diagnostic functions of AI Alter Egos affects the core objective of medical devices law to ensure high quality standards in the healthcare sector, just like the use of AI in the healthcare sector in general. The need for such systems including cost aspects becomes obvious if, for example, in a side-by-side comparison between 157 dermatologists and an algorithm for evaluating skin anomalies, only seven experts are able to make more precise assessments of skin abnormalities than the computer system.[61]

At the same time, the safety-related requirements of medical devices law are also touched upon. These requirements aim for the prevention and elimination of quality defects as well as imminent hazards and risks. The characteristic lack of transparency of algorithmic decision rules (which can produce unforeseen and unpredictable results) as well as the adaptability of continuously learning systems add specific risks to the increased basic risk inherent in all

[57] See CJEU, *Snitem and Philips France* (n 47) para 33.

[58] Cf. for the latter two examples again BfArM, 'Orientierungshilfe Medical Apps' (n 49) point 3.

[59] Cf. also with numerous practical examples in European Commission, 'Medical Devices' (n 46) 17, 18.

[60] See in principle CJEU, *Snitem and Philips France* (n 47) para 36.

[61] Cf. with this very example Y Frost, 'Künstliche Intelligenz in Medizinprodukten und damit verbunden medizinprodukte- und datenschutzrechtliche Herausforderungen' (2019) 4 *MPR* 117, 117.

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

medical devices. Yet, precisely this adaptability is considered particularly attractive in the field of intelligent medical devices. Nevertheless, and in view of the high-ranking fundamental rights to which medical device risks generally refer (life and limb), these specific risks must be taken seriously and addressed appropriately by the regulatory authorities.

Particularly relevant for the development and operation of Alter Egos in the health sector and their basic functions (i.e. indirectly for the individual database function and the collective Big Health Data function, directly for its diagnostic functions) are the structural requirements laid down by the MDR. A look at these structural requirements of medical devices law shows that the introduction of intelligent Alter Egos in the healthcare sector will encounter a legal matter that is already particularly well adapted to the specific technology-related risks of such products for the protected goods concerned.

At the top of structural requirements is the general obligation to ensure the safety and efficacy of the medical device,[62] which is differentiated by further requirements, such as the obligation to perform a clinical evaluation or a clinical trial according to Article 10(3) MDR.[63] For the marketing of intelligent Alter Egos, some of these specifications seem particularly relevant. For example, in addition to the obligation to set up a general quality management system as part of quality assurance, which has been customary for industrially producing companies for decades,[64] the MDR orders the introduction of a risk management system,[65] in the context of which the specific risks of software and data-based products in particular must also be explicitly addressed.[66] In addition, according to Article 10(10) MDR, the 'manufacturer' of the Alter Ego must set up a post-marketing surveillance system in the sense of Article 83 MDR. At least in theory, the typical possibility of unforeseen outputs of AI Alter Egos in general and the adaptability of continuous learning systems in particular can be countered with such systems. In accordance with the regulatory concept of medical devices law, these abstract and general requirements are also specified in more detail for software products by means of special ('harmonized') technical standards. Particularly relevant in this respect is the international standard IEC 62304[67], adopted by the responsible European standardization organization Cenelec, which supplements the risk management standard ISO 14971 with software-specific aspects and also formulates requirements for the development, maintenance, and decommissioning of stand-alone software and for integrated software.[68] In particular, these standards contain, for instance, guidelines for the handling of raw data and its transformation into 'clean data' as well as for the proper training and validation of algorithms.

It is quite likely that that new types of risks are created in the development of intelligent medical devices if AI Alter Egos became actually widely used and were replacing conventional medical services and institutions. Depending on whether and to what extent such scenarios

[62] MDR, Article 10(1) in conjunction with Annex I Chapter I 1.

[63] In addition to these general warranty and risk management requirements, there are also labeling, documentation, recording, reporting, and notification obligations that relate to the warranty and risk management requirements. For reasons of simplification, they will not be discussed further here.

[64] See MDR, Article 10(9) in connection with Annex IX Chapter I. Cf. on the emergence of quality assurance systems from the 1960s onwards and on the principles of quality management in detail F Reimer, *Qualitätssicherung. Grundlagen eines Dienstleistungsverwaltungsrechts* (2010) 115 *et seq.*

[65] MDR, Article 10(2) in conjunction with Annex I Chapter I 3.

[66] See MDR, Annex I Chapter II 17, in particular point 17.2 MDR: 'For products incorporating software or in the form of software, the software shall be designed and manufactured in accordance with the state of the art, taking into account the principles of software life cycle, risk management including information security, verification and validation'.

[67] International Standard IEC 62304 Medical Device Software – Software Life Cycle Processes.

[68] For further relevant standards, see for example the overviews in C Johner, M Hölzer-Klüpfel, and S Wittorf, *Basiswissen Medizinische Software* (2nd ed. 2015) 28 *et seq.*; G Heidenreich and G Neumann, *Software for medical devices* (2015) 260 *et seq.*

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

actually happen and, given the event that these new types of risks are not specifically addressed in the MDR or in other relevant harmonized standards, the corresponding standards can certainly be further developed. Manufacturers and 'notified bodies' (i.e. the certified inspectors of medical devices) are called upon to take account of the special features of intelligent systems in the context of conformity assessment by means of a risk-conscious but innovative interpretation of the regulatory requirements. Such an interpretative approach shall also be undertaken when such requires a specification or perhaps even a deviation of relevant technical standards.[69] It will be possible for instance, to derive certain Good Machine Learning Practices (GMLPs) from the general provisions of the MDR, including the reference to the development and production of software according to the 'state of the art'.[70] According to the GMLPs, for example, only training data suitable for the product purpose may be selected; training, validation, and test data must be carefully separated from each other, and finally, it is necessary to work towards sufficient transparency of the intended output and the operative decision rules.[71] Continuous Learning Systems in Alter Egos are systems with decision rules that can be continuously changed during product operation and therefore actually have AI in the narrower sense and their application may generate specific risks as well. In principle, a change in the decision rules can become legally relevant from three points of view: it can affect the performance, safety, or intended use and/or data input of the product or its evaluation.[72] The manufacturer has to prepare for such changes already under the current regulatory situation, especially since Article 83(1) and (2) MDR obliges him to monitor the system behavior in a way that is adequate for the risk and the product. The manufacturer will have to identify and address (by developing a specific algorithm change protocol) such expected changes already within the scope of the establishment of his risk management system (as pre-specifications).[73] In any case, the distribution of intelligent medical devices does not pose insurmountable difficulties for medical devices law.

However, against the backdrop of the 'general obligation to ensure the safety and efficacy of the medical device' as described and explained above, the restrictions imposed by data protection law on the collection, storage, management, and other processing of health-related information appear to be a possible point of conflict. If restrictions on the use of health-related data, such as limitations on the changes of purpose, prove to be an obstacle to the quality of

[69] A deviation then requires justification, see for example the explicit requirement in MDR, Annex IX Chapter I 2.3, which specifies the test program of an audit procedure by a Notified Body. Cf. on the delicate balance of technical standards between their function of concretizing legal norms on the one hand and the compulsion to design products in conformity with the standard on the other hand, which is to be avoided because it may not be appropriate to the risks and/or innovation, H Pünder, 'Zertifizierung und Akkreditierung – private Qualitätskontrolle unter staatlicher Gewährleistungsverantwortung' (2006) 5 *ZHR* 170 567, 571.

[70] See the formulation in MDR, Annex I Chapter I 17.2. If the harmonized standards do not (any longer) adequately reflect these requirements and a corresponding software product is assessed as compliant, the market surveillance authorities can nevertheless argue that the software product does not comply with the Regulation, as compliance with the standards pursuant to Art. 8 para. 1 MDR only gives rise to a presumption of conformity.

[71] For these examples of GMLPs, see the considerations at M Diamond and others, 'Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device' (FDA, 2019) www.fda.gov/media/122535/download 9–10 (hereafter Diamond and others, 'Proposed Regulatory Framework').

[72] These possible areas of change are already covered in the Medical Devices Regulation, namely in MDR, Annex VI Part C 6.5.2. Almost identical is the information given in M Diamond and others, 'Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device' (FDA, 2019) 6-7 www.fda.gov/media/122535/download, which differentiates between changes regarding performance, inputs and intended use.

[73] For such *SaMD Pre-Specifications* (SPS) and an *Algorithm Change Protocol* (ACP) see Diamond and others, 'Proposed Regulatory Framework (n 70) 10 *et seq.*

https://doi.org/10.1017/9781009207898.031 Published online by Cambridge University Press

outputs for medical purposes, the question arises as to which regime should be given preference in case of doubt. Generalized statements are not helpful here. Rather, these problems should be handled on a case-by-case basis. Of primary relevance is the Alter Ego's concrete medical function specifically affected. In the context of particularly sensitive functions, quality problems or system failures can have particularly far-reaching or even fatal consequences; as in the monitoring of cardiovascular functions or in the diagnosis of serious diseases, any restrictions imposed by data protection law should be overcome by an appropriate interpretation of the legal bases of data protection law. Conversely, a function designed to encourage the data subject to take regular walks should not necessarily be able to access all information, especially highly sensitive information.

IV. CONCLUSION

Overall, my considerations have shown that Alter Egos in the health sector, while appearing somewhat futuristic, already have an appropriate legal framework – at least if it is handled in an appropriate manner that is open to development. The truism will apply: not everything that is technically possible will (immediately) be legally permitted. The creation of a completely 'transparent patient' is (rightly) forbidden in view of the data protection principles of purpose limitation, necessity, and data minimization. Instead, the creation of comprehensive individual health databases in Alter Egos must be carried out step by step. The argument that every health-related data could (in the future) have some kind of medical relevance does not hold water here. On the other hand, data protection law and its legal basis must be interpreted in a way that is open to development and innovation in order to enable medical services that are already feasible and to allow individuals to make comprehensive and effective use of their health data for medical purposes. In order to ensure the quality of these medical functions, the existing rules of medical devices law already provide appropriate instruments that can be easily and adequately applied to AI Alter Egos. Hence, if the existing legal requirements are handled correctly, a responsible and at the same time powerful use of AI Alter Egos in the health sector can go hand in hand.