Wiebke Droste*, Klaus-Peter Hoffmann, Heidi Olze, Werner Kneist, Thilo Krüger, Rüdiger Rupp, Marc Ruta

Interactive Implants: Ethical, legal and social implications

https://doi.org/10.1515/cdbme-2018-0004

Abstract: The use of intelligent implants and prostheses offers significant advances for optimizing medical treatment methods and is combined with an increasing technological modification of human body. This raises many exciting questions concerning law, ethics and social implications: Does the use of these techniques stay in line with our legal system and if yes, can the technical use be limited by governmental restrictions under certain conditions? Have moral values to be incorporated into technical artifacts? If machines are recreated from human beings, do they have to be provided with a legal subjectivity?
Medical devices must be compatible with a high level of protection of health and safety. Therefore challenges, which are consequences of the indeterminate behaviour and the autonomous learning abilities of artificial intelligence, have to be faced. For avoidance of any hazards for legally protected rights medical product manufacturers have to assume legal duties, which affect construction, instruction and product development. For medical professionals there are also liabilities of maintenance measures and technical control that have to be accomplished.
Associated with the use of intelligent medical devices is the processing of personal data on health. Health data have a high potential for misuse and discrimination and therefore they're in need of special protection, particularly with regard to the development of "Big Data", "Ubiquitous computing", "Internet of Things" and constantly increasing cybercrime.
If damages are suffered from the use of intelligent medical devices, difficulties in determining infringing acts, causality and culpability occur, especially because of the missing view into the technical progress of decision-making. It has to be explored, if the current liability law is able to assign responsibility adequately, otherwise there has to be found an appropriate concept for liability.

***Corresponding author: Wiebke Droste**, Institut für Deutsches, Europäisches und Internationales Medizinrecht, Gesundheitsrecht und Bioethik der Universitäten Heidelberg und Mannheim (IMGB), Schloss/Postfach, 68161 Mannheim, Deutschland, e-mail: wiebke.droste@imgb.de
Klaus-Peter Hoffmann, Fraunhofer-Institut für Biomedizinische Technik, Sulzbach, Germany
Heidi Olze, Klinik für Hals-, Nasen-, Ohrenheilkunde, Charité – Universitätsmedizin Berlin, Berlin, Germany
Werner Kneist, Klinik für Allgemein-, Viszeral – und Transplantationschirurgie, Universitätsmedizin Mainz, Mainz, Germany
Thilo Krüger, inomed Medizintechnik GmbH, Emmendingen, Germany
Rüdiger Rupp, Klinik für Paraplegiologie, Universitätsklinikum Heidelberg, Heidelberg, Germany
Marc Ruta, Wilddesign GmbH & Co. KG, Gelsenkirchen, Germany

Interactive implants – therapeutic benefit and IT-Enhancement

According to the legend of Daidalos and Icaros, who tried to escape from captivity from the island Crete by using wings out of feathers and candle wax, human beings have always been striving to enhance their bodies up to attainment of superhuman capabilities. Also nowadays the pursuit of modification and enhancement of human bodies is omnipresent and has already been made to a consumer good. Recently there has been a so called "Cyborg"-movement. The term "Cyborg" describes human beings, who want to upgrade their bodies permanently by using artificial components such as implants, RFID-chips or prostheses to increase their physical, mental and sensual abilities.

The advanced technology of intelligent and interactive implants and prostheses provides the exclusive use for therapeutic purposes as well as the option to enhance physical abilities without the existence of any therapeutic indication. For instance, the integration of information and communications technology offers an individual adjustment of

body function to the environment based on measurement and monitoring of body parameters and thus a continuous optimizing of physical abilities. At this the transitions between the use of the advanced technology for therapeutic purpose and for body enhancement are partly seamless: for example, the insertion of an implant into the cochlea may be useful medically indicated and lead to body improvement at the same time by making ultrasonic and infrasonic waves audible.

These special circumstances raise the question whether and to what extent the increasing advance of technology in human body can be regarded as consistent with human dignity protected through Article 1 (1) GG. The legal discussion concerning this question has already started concerning neuroenhancement[1] and can be transferred to the increasing use of technology in human body: does the use of technology in human body mean a self-manipulation of personal identity and authenticity, that have to be limited by governmental restrictions for the protection of individuals and for the maintenance of human species?[2] Or is the use of technology categorically protected by personal rights in general through Articles 2 (1), 1 (1) GG, so that every restriction has to be justified? The answer to these questions conforms substantially with the concrete form and arrangement of the implant system and its specific application scenario: are there any hazards for the rights of human dignity and self-determination that come from the involvement of information and communications technology because of the eventuality of observation, manipulation or even external control by third persons? What must be the concept for an appropriate implant-system to exclude these risks? This demands a structured overview of the legal requirements laid down in current legislation to evaluate whether and to what extent the use of the implant-system can be considered as appropriate to our legal system.

Challenges of the use of the implant-system

In accordance with Annex I section 1 medical device regulations (MDR) medical devices have to be compatible with a high level of protection of health and safety and must be designed and manufactured in such a way that they will not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons, provided that any risks which may be associated with their intended use constitute acceptable risks when weighed against the benefits to the patient. Thus, medical device manufactures have to figure out through an analysis of benefits and risks whether the risks entailed by the product can be accepted in relation to its advantages. Pursuant to annex I section 4 lit. a-c MDR risks that proceed from medical devices have to be eliminated or reduced according to the principle of embedded safety through safe design and manufacture as far as possible. Where appropriate, adequate protection measures, including alarms if necessary, have to be implemented. Furthermore, manufactures shall inform users of any residual risks.

Networking ICT-implants

In addition to the general risks of active implantable products (infection risks, external influences by magnetic fields, electrical and electromagnetic interferences, radio signal interferences, radiation exposure, heating of energy storage, destruction of implants caused by external factors like accidents or tumbles) dangers that result from the involvement of ICT implants concerning the interconnection with other implant-system components have to be countered: insecure communication links, negative interaction between software and IT environment have to be safely ruled out as well as potential hazards that arise out of constantly increasing cyber-crime. A successful cyber-attack where the attacker succeeding the intrusion into the implant-system enables an extensive potential of manipulation and misuse of the processed data generated by the implant-system. In addition to that a cyber-attack also can lead to functional disorder of the implant-system that in turn can potentially cause personal, material and health damages. In this context especially the integration of patients' own smartphones and tablets presents challenges that have to be met: tablets and smartphones constitute a high potential entry port for malware and cyber-attacks because of their clueless and careless use: the opening of e-mail attachments of unknown senders, careless surfing in open WLAN networks and missing security updates represent a small section of the various strains that have to overcome. To manage this hazardous situation there's a need of a constant and systematic configuration and maintenance of the implant-system to ensure the appropriate and required level of safety at any time.[3] A powerful system management should be able to manage access rights, to add, delete and update software components, to administrate system configuration data and application data as well as to control system components.[4] With respect to this, also patients' own smartphones and tablets have to be considered in continuous maintenance because of their need of constant supply for software-patches and updates. Therefore, particular areas in patients' devices need to be accessible for implant-system administrators whereby it is necessary to ensure by implementing technical

measures that the access is restricted to the categories of administrative operations and no further private data get disclosed in this context.

Artificial intelligence

Through the application of artificial intelligence, the implant-system will be able to adjust its behaviour patterns to the individual and situation-related patients' needs autonomously. Thereby the implant-system is characterized by a permanent and autonomous learning process on the basis of "trial and error". The process of "trial and error" is inevitably associated with flaws which must not lead into intolerable risks for health and safety of patients. This could be provided technically for instance by an encapsulation of the learning capability by separating the motoric execution level from the learning and interaction level, so that learning can take place within previously determined safety areas.[5] It is also conceivable to outfit the implant-system with an additional and separated design of fixed and unchangeable basic functions that can be used in reserve in case of occurring errors to guarantee safety and health protection of patients, users and, where applicable, other persons.

Because of the involvement of artificial neural networks that work according to signal processing of human brain, the process of decision making is hardly possible to determine. If damages are suffered from the use of intelligent implants, it is problematic if not impossible to specify infringing acts, causality and culpability. Therefore, there's a need to consider the enactment of strict liability for intelligent medical devices that provides the attribution of responsibility for the production and use of these products regardless of any culpability.

Data protection law

The implant-system as well as its use have to comply with consisting requests and requirements from data protection law. By the adoption of the European regulation on the protection of natural persons with regard to the processing of personal data and on free movement of such data (DS-GVO) a comprehensive regulation has been enacted that coincidentally requires the implementation of data protection and data security technologies to transform the targets of "privacy by design". The underlying idea of these principles is that data privacy and security can best be ensured by implementing corresponding concepts in programming and construction.[6] In this respect controllers of data processing are in charge to implement appropriate technical and organizational measures to integrate the necessary safeguards into the processing in order to meet the requirements of the regulation and protect rights of data subjects. Controller means according to article 4 (7) DS-GVO the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data. Hereafter controller can be the attending physician, who processes data in the course of therapeutic purposes, and furthermore the manufacturer, fulfilling his obligations of product monitoring and surveillance. In addition to this the patient can be considered to be a controller, if the concrete configuration of the implant-system offers room for determining the purpose and means of the processing. Because data processing in the implant-system mostly proceeds autonomously by the system itself, the significant contribution to implement appropriate technical and organizational measures is going to be required by the manufacturer based on an analysis of the hazards that exist for the right of informational self-determination referring to the concrete and situative data processing. The manufacturer has to arrange the implant-system in a way that enables its use in compliance with data protection laws. The higher the risks, the greater the probability of occurrence and the damage dimensions are, the more extensive measures must be met by the controller.[7]

Risks of data processing arise in the context of the use of the implant system for one thing from the processing of health data, which have a high potential for misuse and discrimination. In addition to that there's a threat of the ubiquitous and partly unnoticeable data processing that comes from the involvement of patients' own devices and their interaction with omnipresent networking computing devices (such as cars, clothes and household objects), so called "internet of things". The comprehensive evaluation of available database by using smart technologies like "Big-Data" even enables to convert anonymous data into high intensive personality profiles.[8] Connecting and combining these data gathered out of different sources provides a deep insight into the medical condition, the personality, lifestyle and even prognoses for the probabilities of disease and sickness of the person concerned.[9] Because of this hazardous situation concerning the right of informational self-determination there's a special need for protection that has to be satisfied by designing the implant-system in accordance with data protection law. For this purpose, it is required to store data without personal references as far as possible from the very first beginning on, which can be technically provided through implementing such measurements that offer the possibility for pseudonymization or rendering persons anonymously. Different pseudonyms should be used for

different purposes of the data processing to prevent the correlation and eventuality of connection between the person and their data. Identification data of users that result from the inclusion of tablets and smartphones, such as IP addresses or device identification (device ID) need to be removed, if these devices are used to transfer data to a managed data exchange platform (e.g. in connection with cloud computing). Data must be transmitted only in encrypted form. Combining data from different processing purposes may only take place if this is essential to the functioning of the implant-system. The app that must be developed for the use of the implant-system has to be protected from third-party access as well as from unauthorized transmission of data caused by other smartphone- and tablet apps that gather data without permission and notice. This could be for example achieved by putting data into data containers and additionally by implementing an appropriate level of password protection. Data protection challenges raised by using the implant-system are tremendous regarding the dynamic development of technology, the current threat level of cybercrime and ubiquitous computing, but can be accomplished by an optimally conceptualized technical data protection.

Author's Statement

Research funding: The authors state no funding involved. Conflict of interest: Authors state no conflict of interest. Informed consent: Informed consent is not applicable. Ethical approval: The conducted research is not related to either human or animals use.

References

[1] Neuroenhancement means the not medically indicated improvement of brain function by using pharmacological, genetical, electromagnetic or other exogenous instruments, see Lindner, "Neuro-Enhancement" als Grundrechtsproblem, MedR 2010, 463.
[2] Lindner, a.a.O., 463, 465.
[3] Bundesamt für Sicherheit in der Informationstechnik (BSI), Grundschutzkatalog (GK), M 2.80, 13. EL Stand 2013.
[4] BSI, GK, M 2.170, 15 EL 2016.
[5] Steil/Krüger, in: Lernen und Sicherheit in Interaktion mit Robotern aus Maschinensicht, S. 61.
[6] Martini, in: Paal/Pauly, DS-GVO, Art. 25, Rn. 10.
[7] Martini, in: Paal/Pauly, DS-GVO, Art. 25, Rn. 37.
[8] Roßnagel/Geminn/Handt/Richter, Datenschutzrecht, 2016, S. XVI.
[9] Deutscher Ethikrat, Stellungnahme zu Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung, S. 9; abgerufen unter http://www.ethikrat.org/dateien/pdf/stellungnahme-big-data-und-gesundheit.pdf, abgerufen am 20.03.2018.