ETHICAL AND LEGAL CONSIDERATIONS OF SMART IMPLANTS

Aleksandar Ivanov
Burgas Free University

Abstract: *As technology progresses, an increasing number of individuals are opting for medical procedures that involve the implantation of electronic devices within their bodies. These procedures range from sophisticated prosthetics like cochlear implants to unregulated RFID circuits embedded in people's limbs, carrying personal data. However, these procedures can pose health and privacy hazards. The absence of a standardized legal framework could potentially lead to detrimental outcomes. This paper reviews current legislation and ethical considerations related to smart implants.*

Keywords: *ICT implants, legal framework, RFID, transhumanism.*

I. Technological overview of body implants

This paper provides an analysis of Information and Communication Technology (ICT) implants, discussing their increasing prevalence, potential health and privacy risks, and the need for comprehensive regulation. In this section a short overview of existing ICT implants is presented. Several types of ICT implants are explained along with their characteristics and use cases.

Radio Frequency Identification, or RFID, is a recent innovation in wireless technology. It allows for the identification of objects equipped with special tags. The identification process relies on three key components working together: the RFID tag itself, an RFID reader, and a back-end database system. The tag communicates wirelessly with the reader, which then retrieves necessary information from the database system through the internet to complete the identification. RFID technology has found widespread applications in areas like electronic passports, tracking assets, toll payments, and even controlling access to areas and buildings. Furthermore, its use for identifying animals has been established for some time, and similar solutions are emerging for human identification. There are two main types of RFID tags: passive and active. Passive tags only respond when a scanner sends them a signal, working like little radio receivers. These are commonly used for things like tracking inventory, nuclear waste, or even cows. Active tags are different. They are tiny radio stations that constantly send out their own signal. This makes them easier to find, but they also use batteries [1]. Another classification considers static and dynamic types of RFIDs. Static systems store fixed information, like a patient's medical history, which can be updated by authorized personnel. Dynamic systems, on the other hand, are more complex. They not only store information but also have sensors to gather real-time data from the environment. This added functionality comes at a cost – dynamic systems require more power than static ones. Newer applications like pet microchips use active tags. In August 2017, Three Square Market (32M) became the first company in the US to offer employees voluntary implantation of RFID microchips. Over 50 employees opted-in [1]. The chip allows for tasks like building access, computer login, and cashless purchases at company markets.

32M sees it as a way to improve convenience for their micro market customers. Additionally, they envision future uses like unlocking phones, sharing business cards, and even replacing passports. Companies in Sweden and Belgium have had similar programs since 2015. BioHax, a Swedish company specializing in implanted microchips, partnered with 32M to provide the chips. Another Swedish company, Epicenter, uses implanted microchips to replace key cards, employee badges, and credit cards for specific functions within their facilities. In Sweden, the active implantation of RFID microchips has seen significant adoption, with thousands of individuals having opted for these devices [1]. While current uses are limited, questions remain about potential future capabilities and how employers might leverage them. The current chips cannot track location in real-time, on or off company premises. RFID systems employ security structures to safeguard user privacy. Hash Lock, a simple scheme using a one-way hash function, solves privacy issues but not tracking. Randomized Hash Lock improves on both but struggles with large-scale applications. Other approaches introduce complexities like increased computational load or data leakage vulnerabilities. The YA-TRAP protocol offers improved security but is susceptible to denial-of-service and replay attacks. Tree-Based Private Authentication provides strong privacy but risks data leakage if compromised. [2] RFID implants also extends beyond medical applications to include entertainment and commercial functions, such as the BajaBeach Club in Barcelona, Spain, which allows patrons to keep an electronic bar tab through a subdermal implant system. The US approved RFID implants in humans in 2004 for medical purposes. Tiny chips placed in the arm store a patient's health data for emergencies. A database (VeriMed) holds this information and participating hospitals can access it. Over 600 people have implants so far. [3]

Smart prosthetics is a promising field of medicine that aims at developing prosthetics that can restore lost functionality and adapt to personal requirements of the patient. The most successful smart prosthetic is the cochlear implant. It is widely adopted for treating severe billateral deafness and in most countries is reimbursed for a group of patients by national programs [4]. Another neurorehabilitation prosthetic is the Argus II system. The Argus II system works by connecting a small camera mounted on a pair of glasses to a tiny array of electrodes implanted on the surface of the retina. The camera captures images, which are then converted into electrical pulses and transmitted to the electrodes. These pulses stimulate the remaining retinal cells, sending visual information to the brain and enabling the patient to perceive patterns of light and dark [5]. These advancements in smart prosthetics demonstrate the potential of technology to improve human health and well-being. However, as this field continues to evolve, it is crucial to address challenges related to device affordability, accessibility, and compatibility with various patient needs.

Brain-computer interfaces (BCI) are systems that allow for devices to be controlled via neural activity [5]. The two major types are invasive (that require surgery) and non-invasive. Invasive BCI rely on arrays of electrodes placed on the cortex of the brain and require surgery. They are used to either record brain activity in certain brain area or for stimulation to treat several conditions (such as Deep Brain Stimulation – DBS – to treat epilepsy). Semi-invasive BCIs use Electrocortigography (EcoG) – signal recording using electrodes placed on the brain cortex, not violating the blood-brain barrier (the semipermeable border that separates the circulating blood from the brain). Non-invasive BCIs use brain scanning technology such as electroencephalography (EEG), magnetoencephalography (MEG), functional magnetic resonance imagery (fMRI) among others. Some ICT implants may be incompatible with these scanning methods, which can pose challenges for diagnostic processes in certain cases [5].

Sensor devices are becoming increasingly miniaturized and biocompatible, allowing them to be implanted directly into the human body. These implants can monitor a variety of physiological data, from heart rate and blood sugar levels to brain activity and muscle movements. Implanted sensors can continuously monitor blood sugar levels in diabetics, heart rhythm in patients with arrhythmias, or pressure within the brain for those with hydrocephalus. This allows for real-time data collection and faster intervention if needed. Beyond medical sensors, there is a growing interest in the so called „biohacking“ or „sensory augmentation“ – the extension of natural perception capabilities by means of electronic sensors. Examples are the implantation of magnetic devices that react to magnetic fields, hence enabling the wearer to detect them too, seismic sensors, humidity sensors, air pressure sensors, ultraviolet sensors, etc. Some devices can combine existing sensory modes into new complex ones. One example is the so called sonocolor perception (combining sound and color). Researchers have tested people with implanted magnets and people with similar magnets placed on their skin. They performed various tests to see how well the subjects could sense different strengths, frequencies, and timings of the magnetic signal [6]. Such studies can help find a suitable tradeoff between invasiveness and utility.

II. Potential risks of smart implants use

Implanting RFIDs carries several potential risks that can be categorized into health, privacy and social concerns.

Health risks of invasive procedures include infection, tissue rejection, migration, EM interference. Here is a detailed list.

- Infection: As with any implantation procedure, there's a risk of infection at the implant site [7].
- Tissue rejection: The body might react to the foreign object, causing inflammation or rejection of the implant (Foreign Body Response – FBR) [8].
- Migration: The implant might move from its intended location within the body, potentially causing damage or needing surgical removal.
- Electromagnetic interference: While unlikely, strong electromagnetic fields could potentially disrupt the functioning of the implant or interact with other medical devices.
- Long-term health effects: The long-term health impacts of RFID implants haven't been fully established, requiring further research.

Privacy risks include unauthorized access to the implants, data breaches, surveillance, forced implantation. Malicious actors could potentially steal personal data stored on the RFID chip or track an individual's movements. Security vulnerabilities in the system could lead to data breaches, exposing sensitive information. That way individuals might lose control over their personal data stored on the implant. There's also a risk of forced implantation for identification or control purposes. Currently, employer-used RFID chips are passive and lack GPS tracking capabilities. However, the future might see the implementation of active RFID chips that could potentially track employee location through GPS or similar systems. Some RFID devices have medical sensors. If their employers get access to that information it can be used in malicious ways. Widespread use of RFID implants could raise concerns about increased surveillance and loss of privacy [1]. Other risks include:

- Digital divide: Access to and benefits of RFID implants might not be equally distributed, potentially creating a digital divide.
- Dependence on technology: Reliance on RFID implants could lead to problems if the technology fails or becomes outdated.
- Reversibility: Depending on the implantation method, removing the RFID chip might be difficult or require surgery.

Many patients are now receiving implantable electronic medical devices, including pacemakers, DBS, cochlear implants, retinal implants, etc. Related risks with these devices are similiar to those with RFIDs - rejection reactions, infection, interference with diagnostic tools (such as MRI, PET, CT scans). Recent research has developed methods to mitigate these risks. In [8] researchers found a new way to prevent FBR from implanted devices. Unlike previous medications that suppress tissue healing, this method uses an inhibitor (MCC950) to target a specific inflammatory pathway (NLRP3) and prevent FBR without hindering regeneration. This targeted approach could significantly improve outcomes for patients with long-term implants.[8] Another approaches make use of zwitterionic materials. They balance positive and negative charges and function as a shield against proteins sticking to surfaces. This „antifouling“ property makes them ideal for implants. Studies show that coating implants with these materials (like phosphorylcholine or carboxybetaine) can significantly reduce unwanted tissue growth and improve implant success [9]. Several other techniques were reviewed in the same paper [9]. DBS is a powerful neurological treatment with risks including infection, bleeding, hardware malfunction, misplaced electrodes, unintended side effects from stimulation, and potential impacts on mood, memory, and cognitive functions.

Assessing risks is very important when implanting devices into the body. Scanning technologies are crucial for this purpose. A new technology called TopoChip has been developed to rapidly assess how tiny patterned surfaces influence human immune cells. This platform uses machine learning to analyze how 2176 different micropatterned surfaces affect the behavior of macrophages, a type of immune cell [10].

Awareness of potential risks related to implants allow for properly addressing them with technical and legal regulations. Next section focuses on the legal and ethical aspects of the matter. Various surveys have been conducted to assess peoples concerns about microchip implantation [11][12]. Some of the expressed concerns are data protection, health risks, control issues (the so called methaphysical dilemma), ease of use concerns, social inequality, lack of knowledge. Researchers have used various technology acceptance models to understand the factors impacting the acceptance of subcutaneous microchips (SMs) in certain populations. Čičević et al.[13] considered the three original components of the Technology Acceptance Model (TAM)—Perceived Usefulness, Perceived Ease of Use, and Behavioral Intentions to Use—and added two external variables, „Health Concerns” and „Perceived Trust.” This model was tested on 100 undergraduate students at the University of Belgrade, Serbia. Descriptive statistics for the five dimensions showed that despite most respondents finding the implantation procedure very painful, the estimates for Perceived Usefulness and Perceived Ease of Use were very high. The authors note that reliance on TAM and the sample composition limit the generalizability of their findings. [13]

III. Legal regulations and social impact

As the use of implantable devices expands beyond medical applications into everyday life, it raises a lot of legal and ethical challenges. This chapter explores these complex issues, examining the regulatory frameworks and moral considerations that govern the deployment of both medical and non-medical implants.

As mentioned, RFID implants raise concerns due to potential privacy issues and non-medical uses. Existing RFID regulations are related to field power, bandwidth, duty cycle and manufacturing quality. In the EU RFID devices primarily operate under the standards set by the European Telecommunications Standards Institute (ETSI) – the standard CEPT/ETSI 302-208 [14] .There is a group of standards ISO/IEC 19794 adresses biometric data such as fingerprints, face, description, etc. If an RFID device handles such data it should comply with these standards [15]. In US the Federal Communications Commission (FCC) Part 15 rules are crucial regulations governing the operation of electronic devices that emit radio frequency (RF) energy, which includes RFID devices [16]. Section 15.247 specifically deals with the operation of intentional radiators, such as RFID systems, operating in the frequency bands 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz. Japan's RFID regulations are managed by the Association of Radio Industries and Businesses (ARIB) [17], under ARIB STD-T108, specifying the use of the 920 MHz to 925 MHz band. Similar regulations include the Wireless Planning and Coordination Wing (WPC) in India [18] and the ACMA Radiocommunications (Low Interference Potential Devices) Class Licence in Australia [19]. All these regulations aim to minimize interference with other wireless communications services and devices, thereby enhancing both operational efficiency and privacy protection. Clinics that perform RFID implantations must obtain informed consent form the implanted idvidiuals verifying their awareness of risks. Insurance is recommended to cover for potential complications. To the authors knowledge there is no universal legal framework to address medical procedures to implant non-medical RFIDs, which is a legal gap that can allow for questionable practices.

The European Union has a standardized system („Conformité Européenne“ - CE marking) for approving medical devices across member countries [20].The European Medical Device Regulation (MDR) is a comprehensive set of regulations enacted by the European Union to ensure the safety and efficacy of medical devices within its member states. Officially known as Regulation (EU) 2017/745, it was adopted in April 2017 and came into full effect on May 26, 2021, replacing the older Medical Device Directive (MDD) and Active Implantable Medical Devices Directive (AIMDD). It aims at ensuring device safety and performance [21]. Before marketing, manufacturers must prove the implant’s safety and efficiency, and a notified body must certify this proof for the CE mark to be affixed [20]. The manufacturer must determine if their implant is a medical product as per MDR, classify it into classes I, IIa, IIb, or III based on its intended purpose and associated risks, and fulfill obligations set forth in Art. 10 MDR, including essential safety and performance requirements, risk management, and clinical evaluation [21]. The MDR introduces a unique device identification (UDI) system to enhance the traceability of medical devices throughout the supply chain. The MDR imposes specific obligations not only on manufacturers but also on importers, distributors, and other economic operators, ensuring every party in the supply chain bears responsibility for compliance. ISO has also launched quality standards covering medical devices. The EN ISO 14971 standard is the central standard for the risk management of medical devices. It explains how the corresponding process must be set up and maintained in detail. Manufacturers of medical devices are required to create, record, implement, uphold, consistently revise, and enhance a Quality Management System (QMS) [21]. By applying the pertinent standard EN ISO 13485, manufacturers can meaningfully fulfill legal requirements and other aspects of the QMS to the greatest extent possible. The clinical evaluation of medical devices aims to assess and demonstrate the clinical safety and performance of the medical device based on clinical data For implants, clinical trials to generate clinical data are, with some exceptions, mandatory. [21]. EUDAMED, the European Database on Medical Devices, is a comprehensive and integrated information system developed by the European Union to enhance transparency and coordination between EU member states in the field of medical devices. It serves as a central repository for information related to medical devices available on the EU market [22]. It is also part of the Regulation (EU) 2017/745 of the European Parliament and of the Council [23].

The US Food and Drug Administration (FDA) regulates medical devices to ensure their safety and effectiveness before they reach the market [24]. Devices are classified based on risk, with Class III being the highest risk category. These high-risk devices, like deep brain stimulators, typically require clinical trials demonstrating safety and efficacy to gain premarket approval (PMA) [25]. However, modifications to existing approved Class III devices may not need new trials if deemed similar enough to the original. Additionally, some older Class III devices can obtain clearance through a different pathway by showing equivalence to a previously approved device. This system ensures a balance between innovation and patient safety by placing stricter controls on potentially riskier medical technology. Most Class II devices require premarket notification 510(k) [26].

There exists a political movement advocating for the legalization of a wide range of implant procedures that augment sensory or motor functions in individuals. Advocates argue for the recognition of these body enhancements as integral parts of the individual’s identity. A precedent for such legal recognition was set in 2004 when Neil Harbison, who has a camera device implanted in his scalp, was issued an ID document that legally acknowledged the device as part of his physical identity. In Germany, an official political party has adopted Transhumanism as part of its platform. Informal communities such as the Cyborg Foundation and Transpecies Society organize activities for individuals interested in body enhancement through smart implants. These communities also provide informational resources through online portals. [27]

Outside the legal aspect, there is also a growing interest in arts, related to sensory augmentation (sometimes regarded as „cyborg art”). Due to installing sensory devices in the body, new types of senses are available to implanted individuals and they allow for new types of art. For example, Harbisons’s device that generates sounds corresponding to colors, accounts for a new type of mixed sense, regarded as sonocolor. Using this sense, Harbison created various forms of sonocolor art – color concerts, sonocolor portraits and others [28]. Other forms of cyborg art are related to seismic perception and magnetic field perception. Example of cyborg art is the work of Moon Ribas, a choreographer who has an implant in her arm that allows her to feel seismic activity around the world. She uses this sensory augmentation to create unique dance performances that are directly influenced by the movements of the Earth [28]. Cyborg art can have cultural impact – from new forms of expression and understanding, expanding the concept of human experience, to raising awareness about body enhancement an addressing sensory impariments in people [28]. Cyborg art raises important ethical and philosophical questions about the nature of identity, the human body, and the intersection of biology and technology. These discussions can influence societal norms and values. As cyborg art pushes the boundaries of what is possible with body modification and sensory augmentation, it can influence legal and regulatory frameworks. Laws and regulations may need to evolve to keep pace with these new technologies and practices.

IV. Conclusions

There is a variety of smart implants that can be used in humans, including medical and non-medical ones. All of them pose some levels of risk in terms of privacy, consent, medical safety and disruption of everyday life. There is no unified global legal framework that address all these issues. Some of the use cases (usually medical) are covered by existing laws and regulations, but others are unregulated and often performed in a DIY fashion. This can be dangerous and increase the likelihood of the mentioned risks occurring in reality. Thus, further efforts to legally address implantation is needed, considering the growing use of these devices.

REFERENCES

[1] Simpson, S.E., Comment: Microchipping employees and privacy implications - does my boss know where I am right now?, *Marquette Benefits and Social Welfare Law Review*: Vol. 20 : Iss. 2, Article 7. Available at: https://scholarship.law.marquette.edu/benefits/vol20/iss2/7, 2019

[2] Ibrahim, A., et al., Review of different classes of RFID authentication protocols,*Wirel. Netw*., 2019

[3] Foster, K., Jaeger, J., Ethical implications of Implantable Radiofrequency Identification (RFID) tags in humans, *The American Journal of Bioethics,* 8:8, 44-48, DOI: 10.1080/15265160802317966, 2008

[4] Ivanov, A., EU policies on cochlear implants, *Бургаски свободен университет - Юридически сборник*, Том XXX [BG], ISSN 1311-3771, 2023

[5] Ivanov A., A review of brain-computer interfaces and their applications. Electrotechnica & Electronica (E+E), Vol. 58 (4), 2023, pp.100-105, ISSN: 0861-4717 (Print), 2603-5421 (Online), 2023

[6] Harrison, I., Warwick, K., Ruiz, V., Subdermal magnetic implants: an experimental study, *Cybernetics and Systems*, 49:2, 122-150, DOI: 10.1080/01969722.2018.1448223, 2018

[7] Schiffmann A, Clauss M, Honigmann P. Biohackers and self-made problems: infection of an implanted RFID/NFC chip: a case report. *JBJS Case Connect.* 10(2):e0399. doi: 10.2106/JBJS.CC.19.00399. PMID: 32649126., 2020

[8] Barone, D.,et al., Prevention of the foreign body response to implantable medical devices by inflammasome inhibition, https://doi.org/10.1073/pnas.2115857119, 2022

[9] Capuani, S., Malgir, G., Chua, CYX, Grattoni, A., Advanced strategies to thwart foreign body response to implantable devices. *Bioeng Transl Med.* 2;7(3):e10300. doi: 10.1002/btm2.10300. PMID: 36176611; PMCID: PMC9472022. 2022

[10] Unadkat, H. & H., et al., An algorithm-based topographical biomaterials library to instruct cell fate. *Proceedings of the National Academy of Sciences of the United States of America.* 108. 16565-70. 10.1073/pnas.1109861108. \2011

[11] Shafeie, Sh., Chaudhry, B., Mohamed, M., Modeling subcutaneous microchip implant acceptance in the general population: a cross-sectional survey about concerns and expectations. *Informatics.* 9. 24. 10.3390/informatics9010024., 2022

[12] Žnidaršič, A, A. Baggia, et al., Are we ready to use microchip implants? An international cross-sectional study, *Organizacija,* vol. 54, no. 4, pp. 275–292, doi: 10.2478/orga-2021- 0019 , 2021

[13] Davis, F.D., Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* 1989, 46, 319–340.

[14] https://www.etsi.org/deliver/etsi_en/302200_302299/302208/03.03.01_60/en_302208v030301p.pdf

[15] https://webstore.iec.ch/preview/info_isoiec19794-5%7Bed1.0%7Den.pdf

[16] https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15

[17] https://www.arib.or.jp/english/

[18] https://dot.gov.in/spectrum-management/2457

[19] https://www.acma.gov.au/licences/low-interference-potential-devices-lipd-class-licence

[20] https://single-market-economy.ec.europa.eu/single-market/ce-marking_en

[21] https://biomatdb.eu/2022/10/27/approval-of-medical-implants-according-to-the-european-medical-device-regulation-mdr/

[22] https://webgate.ec.europa.eu/eudamed/landing-page#/

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745

[24] https://www.fda.gov/medical-devices

[25] ttps://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpma/pma.cf

[26] https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpmn/pmn.cfmh

[27] https://hpluspedia.org/wiki/Main_Page

[28] https://www.cyborgarts.com/