STUDIA PRAWNICZE. Rozprawy i Materiały 2025, nr 1 (36)
STUDIES IN LAW: Research Papers 2025, No. 1 (36)
e-ISSN 2451-0807 • ISSN 1689-8052
DOI: 10.48269/2451-0807-sp-2025-1-12

Patrycja Kornacka
MA, Andrzej Frycz Modrzewski Krakow University
orcid.org/0009-0007-6051-3130
patrycjakornacka15@gmail.com

Cybernetic implants in non-medical applications. Selected aspects

Introduction

There are spheres in our lives that will always be accompanied by serious problems and challenges, and health is one of them. Human tissues and organs wear out and age over the years, and the human body is unable to regenerate itself to its original state. Moreover, in a situation where strategic organs in our bodies begin to deteriorate there are slim chances of sustaining the patient's life. Consequently, in many situations traditional solutions are no longer sufficient, hence more and more innovative solutions based on information and communication technology (ICT)[1] are being developed. In this text we will look at one of them – medical implants. The dynamic development of ICT applications in medicine has resulted in the perception that ICT has the potential to be used in non-medical areas as well.

Implants in medicine

The priority of the modern approach to treatment is to improve the quality of life of the sick, which involves expanding their

[1] ICT – Information and communication technologies.

independence and self-reliance. Currently, various types of prostheses or implants, which can be described as 'repair' devices, are widely used in medicine[2]. At this point it is worth clarifying the term implant. An implant (interchangeably referred to as an implant) is a foreign body that is implanted into the body to restore natural functions or improve the aesthetic appearance of the patient. They permanently connect to living tissue or participate in its regeneration. However, in recent years, in addition to the medical applications of implants, a path has gradually developed that aims to use the above tools to enrich and expand the skills of a healthy person. An example of the use of such devices is ICT implants. They represent implants that have been created through the use of information and communications technology. They are often interchangeably referred to as ICT, information technology or information and communications technology. Their task is to process, collect and send data in electronic form using any available electronic communication tools or digital techniques. In other words, it is a foreign body, stably connected to the human body, containing elements of ICT, which is introduced for a specific purpose. This device contains software that allows it to communicate with the outside world and transmit data to it.

ICT implants have very broad applications in clinical practice. They form a bond that connects the body with technology, and their use is primarily related to helping a defective organ or organ work or improve its performance. The main task is to improve the comfort of life and control the patient's health without the physical presence of a doctor. We can distinguish several groups of implants. Some of the most commonly used include:

– A pacemaker, which is responsible for regulating the heart's rhythm by delivering electrical impulses to the heart. Its function is to prevent the heart from working unevenly or too slowly. In recent years, as a result of numerous modifications, it has become a more sophisticated tool, with integrated sensors that adjust output based on estimated demand and communicate via

2 *Organs*, European Commission, health.ec.europa.eu/blood-tissues-cells-and-organs/organs [accessed: 12.03.2025].

RF[3] with the outside world – these are IMDs[4], which have been in use for decades. Data can be sent to the implanted device, for example, to trigger a particular action on demand.

- Cardioverter-defibrillator (ICD), responsible for monitoring the heart rhythm, and in case of sudden cardiac arrest provides defibrillation. It is generally used for patients at risk of sudden death caused by ventricular fibrillation. It can detect arrhythmia and also stop it.
- Neuroimplants, are used to treat neurological diseases, such as Parkinson's disease, dystonia, for example. They are used for deep brain stimulation (DBS), making them the broadest in scope. A device is implanted that sends electrical impulses to a specific part of the brain. This device contains an electrode with 4 or 6 cylindrical electrodes at different depths connected to an impulse generator (IPG). In some areas of the brain, only neuroimplants have been shown to be effective in treating neurological disorders.
- Hearing prosthesis (cochlear implant), its purpose is to restore the function of the lost sense. It is the most sensory nerve prosthesis, as it stimulates the evocation of patterns of nerve fiber activity using a linear array of electrodes inserted into the cochlea of a deaf person, which is the biological receptor for sound.
- Prosthetic lower limbs, allow movement for people who have lost their natural limbs. An example incorporating microprocessors that are responsible for controlling the knee joint and its flexion, resulting in natural movement, is the C-leg[5].

Implants that 'enrich' humans

As for the non-medical use of implants, they are now, most often, used for individual body modification that involves body

---

[3] Radio Frequency – wireless communication, in which radio signals are used to transfer data between devices.

[4] IMDs (Implantable Medical Devices) – an improved pacemaker implant that, among other things, uses communication with the outside world in its operation.

[5] M.B. Popović, *Biomechanics and robotics*, New York 2013, p. 232.

enhancement: from minor cosmetic improvements to more radical changes in appearance and body function. More recently, ICT implants have found their way into facilitating everyday life, with an example being implants located in the hands, in the form of microchips that allow cashless transactions.

Identification of physical objects is based, among other things, on RID[6] technology, which was originally designed to automatically detect physical objects. This was done by means of a small RFID reader device, which was attached to the object in question and thus sent identification data (a sequence of pulses representing a unique code) using radio waves. This gained increasing popularity and recognition, so the use of RFID technology spread to other branches of life, such as logistics, manufacturing, but also defense and agriculture.

This development led to the creation of RFID implants, which are inserted directly into the human body. Anyone can have them, regardless of health status. They take the form of tags or transponders that contain an integrated circuit within them. They have been commercialized and their main task is to facilitate identification and authentication of individuals. They are called 'passive tags' because their operation depends on using the energy emitted by an external RFID reader. What this means is that they do not have an internal power source, and in addition, they have no moving parts in them, making them maintenance-free[7]. The implant represents the unquestionable authenticity and reliability of the person being identified, which is strictly assigned to the individual, unlike biometrics, which can give erroneous results. Another advantage is that it cannot be lost, let alone stolen. Due to their small size, these devices are discreet and unnoticeable to third parties, however, at the same time, by doing so, they limit the efficiency and range of communication.

The use of ICT implants is already being practiced on a large scale in non-medical aspects, in particular, this includes automatic

---

6 Radio Frequency Identification Technology.

7 K. Warwick, M.N. Gasson, *Practical experimentation with human implants*, [in:] *Uberveillance and the social implications of microchip implants: emerging technologies*", eds M.G. Michael, K. Michael, Hershey 2013, pp. 69–84.

payments, controlling access to objects or identifying physical objects, and with ongoing research and new discoveries, their use will only increase.

Risks associated with the proliferation of ICT implants

Human enhancement technologies raise a number of concerns, primarily related to safety in the broadest sense. Undoubtedly, interfering with the human body by introducing elements resulting from the development of technology and information technology is an extremely dangerous activity. It is clear that as technology, and consequently implants, continue to develop, related to the improvement and enrichment of organ capabilities, the temptation for humanity to use such a solution will increase. Some scientists point to the possibility of creating a symbiosis between man and machine. By permanently, and bi-directionally, linking the motor channels of these entities, man will be able to use the power of machine intelligence and its technological capabilities[8]. This, in turn, carries a great risk of excessive interference with the biological and natural design of the human being. The desire to improve one's organism can lead to situations in which this, healthy individuals, disregarding the possible dangers and threats, will repeatedly introduce foreign elements into their bodies, just to have more skills. And this can lead to a change in the very essence of people. At present, some have already postulated that the era of transhumanism[9] is coming, and its proponents want to radically modify their bodies along the lines of cyborgs. In addition, they expect legal systems to introduce regulations that will allow legal body transformations, in any direction they choose.

---

8 *Human ICT implants: technical, legal and ethical considerations*, eds M.N. Gasson, E. Kosta, D. Bowman, Hague 2012, p. 32.

9 S. Singh, *Transhumanism and the future of humanity: 7 ways the world will change by 2030*, 20.11.2017, forbes.com/sites/sarwantsingh/2017/11/20/transhumanism-and-the-future-of-humanity-seven-ways-the-world-will-change-by-2030 [accessed: 12.03.2025].

A significant threat to the use of ICT implants is the breach of protection or misuse of personal data. Currently, medical implants, where, data leakage may involve sensitive information, i.e. related to health status, are exposed to such a danger. This data belongs to a special category of personal data, since it contains, not only, relevant information about the general state of health, but also that obtained during registration for health care services or during its provision[10]. In possession of sensitive data, it can be used against a person. As implants process huge amounts of information, they are vulnerable to all sorts of incidents[11] that, in the worst case scenario, can lead to a hacked device, with hacking being understood as "the act of identifying and then exploiting vulnerabilities in a computer system or network, usually to gain unauthorized access to personal or organizational data"[12]. While still intercepting a device will involve less invasive implants, hacking a neural implant that connects to the brain, and thus involves the entire body, can lead to serious damage[13]. Equally dangerous are 'denial of service' attacks or the introduction of malware that will lead to the cessation of proper operation of the implant[14]. This issue has been highlighted by Gasson and Koops, among others. They argue that implants that are closely

10 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), Official Journal of the European Union, L 119, 4.05.2016.

11 Incident – any event that has an actual adverse impact on the security of networks and information systems, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union, Official Journal of the European Union, L 194, 19.07.2016.

12 *What is hacking*, kaspersky.com/resource-center/definitions/what-is-hacking [accessed: 12.03.2025].

13 N. Hines, *Neural implants could let hackers hijack your brain*, 6.08.2016, inverse.com/article/19148-neural-implants-could-let-hackers-hijack-your-brain [accessed: 12.03.2025].

14 Z.P. Birnbaum, *Regulating the cyberpunk reality: private body modification and the dangers of 'body hacking'*, „Journal of Business & Technology Law" 2021, vol. 16, issue 1, pp. 119–145.

connected to the human nervous system may be at much greater risk of cyber attacks[15]. The consequence of an attack could be an increased risk of false memory implantation[16] or the appearance of sensory hallucinations[17]. Auditory hallucinations by hackers using popular deepfake video productions are also possible.

A particular risk of cyber attacks arises when a device connects to multiple public and not necessarily secure communications networks. A 'publicly accessible communications network' is defined, according to Article 2(8) of the EECC[18], as a network used wholly or mainly for the provision of publicly available electronic communications services that supports the flow of information between network endpoints. The lack of adequate security and the possibility of making personal information public can lead to identity theft or the use, illegally acquired, of personalities for criminal purposes. So no matter what type of communications network it is and to whom it is shared, the confidentiality of communications should always be assured. The European Group on Ethics in Science and New Technologies (EGE) has created a set of principles that should guide the introduction of ITC implants. Among them were such requirements as data minimization, definition of proportionality, purpose and adequacy, human integrity and autonomy.

The introduction of such advanced technology puts pressure on the creation of sufficiently strong, comprehensive security measures to ensure confidentiality, protect personal data, as well as the implants themselves. Security systems should be impossible to break. Tests conducted on current implants, including a cochlear

---

15 M.N. Gasson, B.J. Koops, *Attacking human implants: a new generation of cybercrime*, „Law, Innovation and Technology" 2013, vol. 5, issue 2, pp. 248–277.

16 P. Perry, *Scientists discover how to implant false memories*, 15.06.2016, bigthink.com/surprising-science/scientists-have-discovered-how-to-implant-false-memo [accessed: 12.03.2025].

17 N. Hines, *Neural implants…*, *op. cit.*

18 EECC – European Electronic Communications Code. Directive (EU) 2018/1972 of the European Parliament and of the council of 11 December 2018 establishing the European Electronic Communications Code, Official Journal of the European Union, L 321, 17.12.2018.

implant[19] and a pacemaker[20], have proven that it is possible to hack into the systems of these devices and take control of them. Particularly vulnerable to cyberattacks is the pacemaker, which in the studies conducted was not immune even to attack by amateur hackers. In 2004, Gartner published several reports that testified that RFID is highly insecure, and can be read and even written to by almost any reading device or smartphone. It also raises the possibility of cloning[21], let alone hacking. This, in turn, is not an optimistic forecast for the future related to cyber threats. That's why it's important to conduct a multifaceted risk assessment in the context of further development of ICT implants.

The issue of liability for insufficient protection of personal data is also problematic. In the event of their leakage, who will be held liable? In the traditional model, it was assumed that the owner of the cyber network was responsible. In contrast, in the new model-GDPR-more emphasis is placed on individuals, i.e. the direct owners of the data. The European model, on the other hand, is based on a multi-faceted approach and differentiates the responsibility of entities. One can still point to the hybrid cyber model, in which responsibility is distributed between the network owner and the implant manufacturer. To sum up, clear and precise guidelines are required on this issue as well, indicating who is responsible for failure to meet and comply with security requirements.

The next likely threat posed by the large-scale use of ICT implants is the issue of dividing society into 'richer' and 'poorer' classes. It is therefore a matter of social justice, which may be disrupted. The concept itself is difficult to define clearly. However, we can assume that under this term should be understood objective and equal criteria for assessing both rights and obligations, as well as

19 N. Hines, *Neural implants…*, *op. cit.*; M.B. Nierengarten, *Protecting medical devices against cyberthreats*, 24.09.2017, enttoday.org/article/protecting-medical-devices-cyberthreats [accessed: 12.03.2025].

20 B. Curley, *Hackers can access pacemakers, but don't panic just yet*, 13.04.2019, foxnews.com/health/hackers-can-access-pacemakers-but-dont-panic-just-yet [accessed: 12.03.2025].

21 J.D. Halamka, A. Juels, A. Stubblefield, J. Westhues, *The security implications of VeriChip cloning*, „Journal of the American Medical Informatics Association" 2006, vol. 13, no. 6, pp. 601–607.

the treatment of certain groups. If this were the case, there would not only be social stratification, but also a widening gap between developed countries and the rest of the world. The degree of affluence could become a factor in determining who will own and how many improvements, as well as how wide their access to functions will be. These individuals, will become more attractive to employers. The use of implants to enrich our abilities and skills will lead to a situation in which all-natural individuals who do not use such devices will be discriminated against and even stigmatized and seen as 'inferior', or conversely, it will be the 'enriched' individuals who will be regarded as such, as long as they are in the minority. Harassment can be a massive problem that will be very difficult to combat and will escalate into social exclusion, which can go even further and include exclusion from certain public services or even health care. Moreover, as Bockman notes: "Moreover, due to the often significant costs associated with HET, wealthy individuals will have greater access to the benefits of improvements, and the resulting unequal distribution of increased opportunities will perpetuate and exacerbate wealth disparities"[22]. In addition to the risks described, Perakslis[23], listed the following risks associated with the use of implants:

- Insightfulness – devices can pry into human behavior on many levels;
- Unintelligibility – unclear or dynamically changing regulations will leave the user unaware of who owns their data;
- Inerasability – the digital history of our behavior is likely to be preserved, and network moderators will have access to it;
- Intrusiveness – as technology develops, it may come to pass that devices will also be able to predict our intentions, not just our behaviors;
- Obscurity – holders will not be fully aware of what data is stored, by whom, for how long and for what purposes it may be used;
- Involvement – the use of technology is becoming a requirement for participation in society.

---

[22] C.R. Bockman, *Cybernetic-enhancement technology and the future of disability law*, „Iowa Law Review" 2010, vol. 95, no. 4, p. 1315.

[23] C. Perakslis, K. Michael, *Ethical issues to consider for microchip implants in humans*, „Ethics in Biology, Engineering and Medicine: An International Journal" 2012, vol. 3, no. 1–3, pp. 75–86.

Access to ICT implants should therefore be based on real needs, not economic resources. In the long run, there may even be situations where human rights will be granted only to enhanced persons or even androids, which already perform human activities and are created in the shape of human beings. Undoubtedly, such a situation would lead to the demise of humanity as naturally biological beings. That is why it is so important to introduce regulations that would define for what non-medical purposes implants can be used and create appropriate restrictions on their excessive use.

Non-medical use of ICT implants under the law

Work related to HET (Human Enhancement Technologies), as well as the upgrading of ICT implants, is generating considerable controversy, particularly on ethical and legal grounds. One of the most important questions raised in connection with the non-medical use of ICT implants is their impact on humanity and its rights. Is the proliferation of such implants safe for basic human rights and society, and will this not lead to increased control over citizens, limiting their rights and freedoms? The clinical use of ICT implants is regulated in some way, and as a result there are no objections to this, an example being the pacemaker. However, the same cannot be said of implants inserted into the body for non-medical purposes, which additionally have access to digital networks, as there is no regulation here. If misused, they can pose serious risks to the individual, for example, becoming a tool of social surveillance or manipulation. As a result, this poses a potential threat to human dignity and undermines the foundations of a democratic society. In addition, in the case of neuroimplants, which directly affect the nervous system, threats arise to individual autonomy and subjective individuality. Indisputably, these aspects raise serious questions.

According to the demands of the European Group on Ethics in Science and New Technologies, the use of human enhancement technologies should be done in accordance with respect for basic human rights, as well as respect for human dignity[24]. This is because

[24] Z. Warso, S. Gaskell, *Sienna D3.2: analysis of the legal and human rights requirements for Human Enhancement Technologies in and outside the EU*

a set of basic human rights is the foundation on which all other legal regulations should be made. They are intended to protect individuals and ensure their dignified existence. Nevertheless, there is still a lack of clear and precise legislation to regulate the use of HET. Thus, it is in vain to look for them, since all we can find are general, basic requirements for the safety of a given product, as exemplified, for example, by the European Medical Devices Directive[25]. However, it makes a clear distinction between which devices are intended for medical purposes and which for use by healthy people. This boundary, is drawn by making a division based on how manufacturers market their devices. Thus, devices marketed for 'therapeutic and/or diagnostic' purposes are regulated by the MDD, while those aimed at healthy individuals are excluded from it. It is worth mentioning that the EGE also makes a distinction between implants, indicating their purpose, while stipulating that non-medical implants are not explicitly covered by existing legislation[26]. In view of this situation, work began on changing the legal system, which manifested itself in Regulation (EU) 2017/745[27] of the European Parliament and of the Council, establishing stricter regulations that had to be met in order to authorize medical devices, as well as those non-medical ones indicated in Annex XVI. In the absence of harmonization of standards for non-medical devices, they would have common specifications with similar medical devices. Eventually, the Regulation

[WP3 – *Human enhancement: ethical, legal and social analysis*], 2019, https://doi.org/10.5281/zenodo.4066616.

25 MDD – European Medical Devices Directive: Directive 93/42/EEC of 14 June 1993 concerning medical devices, European Parliament and the Council, Official Journal of the European Communities, L 169, 12.07.1993.

26 Ethical aspects of ICT implants in the human body: opinion presented to the Commission by the European Group on Ethics, MEMO/05/97, Brussels, 17.03.2005, p. 35.

27 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, Official Journal of the European Union, L 117, 5.05.2017.

of the European Parliament and of the Council (EU) 2023/988[28] on general product safety was created[29], to be applied from December 13, 2024. This document is a new, but above all, a key instrument within the EU legal system. Taking into account the level of development of technologies, risks and dangers of new technologies, the regulation introduced clear and detailed provisions that leave no room for transposition by member states. In the main, the act is intended to act as a 'safety net' for consumers, who are entitled to safe products, and is also intended to provide a rapid warning system for unsafe products. GPSR introduces or modernizes, among other things, such provisions as those relating to the definition of 'product', online sales, safety assessment, and product traceability and identification rules. In short, it can be said that GPSR marks a profound revision of product safety regulations in the European Union. The European Union Legal Affairs Committee's Recommendations of May 4, 2020, containing draft rules governing AI tort liability, also play an important role in shaping future AI regulations.

The issue of liability for ITC implants

The lack of regulation of medical and product liability poses many problems and inaccuracies, as it is unclear who should be liable for any defects. Theoretically, this aspect is a matter of national law. As this is a very broad issue only selected aspects will be touched upon without going into a detailed polemic. Difficulties in establishing product liability, among other things, are due to the fact that it has not been clarified what 'defective' means in the case of ITC implants. It can be both the absence of an effect and the occurrence of an effect that was not intended, but does not in itself lead to negative

[28] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, Official Journal of the European Union, L 135, 23.05.2023.

[29] GPSR – General Product Safety Regulation.

consequences[30]. With regard to current EU as well as national regulations, in the case of a defective product, one can demand, among other things, its replacement or repair, which for some ITC implants may be unfeasible. It is also extremely important to demonstrate a cause-and-effect relationship, which even here poses many difficulties due to the complexity of the components of ITC implants. Following the implementation of Council Directive No. 85/374/EEC of July 25, 1985[31], a model of liability for dangerous products was adopted, which is based on the principle of strict liability. It was included in the European Parliament's Resolution of February 16, 2017, containing recommendations to the Commission on civil law provisions on robotics[32], where manufacturers of AI systems should be liable on a strict liability basis. Thus, it seems to be a rational solution, as the manufacturer is obliged to meet all safety standards, which is emphasized in both EU and national regulations, in Article 4491 § 3 of the Civil Code[33]. And if he failed to do so, he should be liable regardless of fault, according to the principle of *cuius commodum eius periculum*.

The issue of medical liability is much more complicated. In the first place, one should look at the question of whether one can speak of medical liability in the case of the use of ITC implants that are not based on medical indications[34]? Looking at it rationally, regardless of an individual's intentions, the insertion of an implant

30 *Human ICT implants…*, *op. cit*., pp. 69–79.

31 Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), Official Journal of the European Communities, L 210, 7.08.1985.

32 European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL)), Official Journal of the European Union, C 252, 18.07.2018.

33 Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny [Civil Code], Dz.U. [Journal of Laws] 2024, poz. [item] 1061.

34 K. Bączyk-Rozwadowska, *Odpowiedzialność cywilna za szkody wyrządzone w związku z zastosowaniem sztucznej inteligencji w medycynie*, „Przegląd Prawa Medycznego" 2021, t. 3–4, pp. 45–60.

into the body requires a more or less complex procedure, and this in turn falls within the framework of a medical procedure. Going further, the next question that arises is whether the doctor or doctor dentist, will be able to perform the aforementioned procedure? At this point, it is worth communicating another aspect that is related to the demands made, namely, can AI be given legal subjectivity? This is important insofar as, depending on this, one can consider whether AI could be held liable?[35]

However, accepting the view of AI's lack of subjectivity, it seems that the *de lege ferenda* postulate specifying that only the authorized person to carry out the non-medical procedure involving the implantation of an ITC implant will be a specialist: a doctor or a doctor-dentist, is appropriate. This, in turn, makes it possible to define the framework of liability for the damage caused, which will be borne by the operator, i.e. the aforementioned doctor or physician-dentist. Assuming the adopted model, the operator would bear civil liability on the basis of fault, which would have to be proven or presumed. Liability *ex delicto* has a general reference when the resulting damage is due to improper or inadequate use of the object. The European Parliament, in its Resolution of February 16, 2017, 2015/2013(INL), constructed a just demand to establish the minimum professional requirements to be met by the operator during implantation. Based on the aforementioned document, only the person who knows or should know of the revealed danger will be liable on a fault basis. Thus, liability will be borne by the one who violated the legal duty to prevent the danger. It is also important to indicate the scope of information that the specialist should provide to the patient before the procedure.

Ethics and the era of transhumanism

In the context of the era of transhumanism vs. human dignity, two basic trends have developed, namely: "the first assumes that cyborg dignity will surpass human dignity, while the second assumes

[35] P. Księżak, *Prawo cyborgów (2). Własność i dobra osobiste*, „Głos Prawa. Przegląd Prawniczy Allerhanda" 2022, t. 5, nr 1(9), poz. 12, pp. 45–60.

that cyborgization deprives of dignity"[36]. Undoubtedly, both of the aforementioned positions may be correct. However, it is first necessary to ask what human dignity, which is considered the basis of all rights, actually is.

Human dignity is an inherent and inseparable part of every human being. It is a universal condition to which the legal order must be subservient. This value is so important that it was already mentioned in the preamble of the Universal Declaration of Human Rights[37]. Many legal acts of international or European stature are based on the concept of human dignity, while emphasizing its primary role in the formation of all law. The principle of respect for human dignity implies the right to autonomy and self-determination of the individual.

It is difficult to unequivocally answer the question of what human dignity is, because it is an ambiguous concept. For the purposes of consideration, we can assume that it is "a person's inner conviction of his moral and ethical integrity and honor, as an expression of the positive attitude of other people to his personal and social worth"[38]. Human dignity prevails over autonomy, ensuring its proper protection. It is based, above all, on self-esteem and expectations of respect[39].

As a result of the rapidly developing close human-machine[40] relationship, it is so important to lay the foundation for an ethical

---

36 M. Klichowski, *Edukacja cyborgów. Jak działać, by nowe technologie były sprzymierzeńcem, a nie wrogiem?*, Poznań 2015, p. 436; M. Łątka-Płachta, *Cyborgizacja a zasada równości, prawo do samostanowienia o sobie oraz zasada godności*, „Progress Journal of Young Researchers" 2022, vol. 11, pp. 127–146.

37 Universal Declaration of Human Rights – a set of human rights and principles for their application, adopted on 10 December 1948, France, United Nations Document A/RES/217(III).

38 Wyrok Sądu Najwyższego [Supreme Court Judgment] z 21.03.2007, I CSK 292/06, Legalis nr 156746.

39 B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012, nb 2.

40 European Commission: Directorate-General for Research and Innovation and European Group on Ethics in Science and New Technologies, *Statement on artificial intelligence, robotics and 'autonomous' systems – Brussels, 9 March 2018, Publications Office*, 2018, data.europa.eu/doi/10.2777/531856.

system that, together with the legal system, can harmoniously regulate cybernetic implants. Morality is a difficult issue insofar as, based on the basic framework of ethics, the individual is entitled to an individual perception of what is acceptable or unacceptable, what is right and wrong. In turn, certain discrepancies may arise from this, which have no place in the context of ICT implants.

Undoubtedly, the construction of the ethical aspect should include the three basic values of dignity, autonomy and moral responsibility. Again, it should be emphasized that dignity guarantees autonomy, and this in turn translates into the creation and setting of an individual's own standards or goals in life. The cognitive processes taking place

> […] are among those most closely identified with the dignity of the human person and human agency and action par excellence. They usually carry the qualities of self-awareness and causality, based on rationale and values. Autonomy in the ethically relevant sense of the word can therefore only be attributed to human beings[41].

Accordingly, dignity as well as autonomy are closely linked to the human being, i.e. the subject, rather than the object, which is undoubtedly the implant. Moreover, the autonomy of a human organism is not equal to that of an artificial intelligence, which is a system to develop its own pattern of decisions. Therefore, the two phenomena cannot be equated. Moreover, cybernetic implants incorporating artificial intelligence cannot limit the freedom of humans to determine their own standards.

Turning to further analysis of the matter at hand, can ITC implants integrated into the human body also become human structural elements? As you can see, another issue arises here that requires proper analysis, and perhaps going beyond the previous civilist dichotomous classification of subject – object. At this point, the intimate relationship between bodily and mental functions is the basis of our identity. But what if an object with its own intelligence appears inside the human body? Undoubtedly, a notable issue here is the degree of integration as well as automation

---

[41] *Ibidem*, p. 9.

of the cybernetic implant with the human body. At this point, it is worth quoting the conclusions of M. Quigley and S. Ayihongbe,

> the greater the physical integration of [things] with individuals, the greater the support or replacement of bodily functioning, or the greater the dependence of individuals on devices, the more the subject–object dichotomy is blurred and shattered. Significantly, this division is completely eliminated in the case of life-support devices[42].

Adopting the view of the subjectification of the object (the ITC implant), one can conclude that, in such a case, personal rights would also extend to cybernetic implants. Following this line, although the implant would constitute a subject, this would not mean that it is the same as a human being. This is because there would still be two separate decision-making systems in operation – the biological human being and the AI contained in the implant. Thus, it is reasonable to ask the question of whether there would still be full autonomy of the individual, or whether the cybernetic implant would thus violate it? How to make a clear separation between the two? Studies conducted on brain implants that were created to alleviate Parkinson's disease show that ITC implants can affect the nervous system, particularly the brain. Thus, they affect the identity of humans as a species and their autonomy. What, then, in a situation of opposing decisions? Who will have a real influence on the final intention?

Closely related to the above topic is also the issue of the right to preserve bodily integrity. Related to this is the aforementioned problem of the blurring of the scope of meaning of the boundary of the body. In view of the technological changes taking place, it is becoming unclear. This is due to the fact that the implant begins to be perceived as a part of the body, so that any technological improvements fall within the meaningful scope of 'body' as a biological creation[43]. This, in turn, leads to a change in the concept of the body,

---

42 M. Quigley, S. Ayihongbe, *Everyday cyborgs: on integrated persons and integrated goods*, „Medical Law Review" 2018, vol. 26, issue 2, p. 306.

43 M. Gruchoła, *Wartość ciała biologicznego i ciała humanoida w świetle założeń teologii ciała*, „Kultura Słowian. Rocznik Komisji Kultury Słowian PAU" 2023, t. 19, pp. 215–227.

and thus a change in the perception of certain rights, an example of which is bodily integrity, autonomy.

Bodily integrity is mentioned, among other things, in Article 3 in the EU Charter of Fundamental Rights[44]. A distinction is made between physical integrity and mental integrity. It can be understood in two ways, firstly, as the right to do anything with one's body that is not forbidden – but this must come from the conscious decisions of the individual; secondly, as protection against unlawful, harmful interference with our bodies by third parties. Bodily integrity is particularly assured in the fields of medicine and biology. Therefore, in order to implement any activities that violate bodily integrity, it is necessary to give consent, by which is meant a voluntary, specific, informed and unambiguous demonstration of the individual's will. On the other hand, in a situation where ICT implants are introduced into our bodies, there may be a problem with autonomy due to the existing risk of artificial intelligence making decisions or infecting the software by third parties.

More broadly, the use of HET can lead to violations of the right to privacy and family life. These rights are listed in the European Convention on Human Rights[45], the International Covenant on Civil and Political Rights[46], among others. Private life should be understood as the physical as well as moral integrity of an individual, sexual life, medical treatment and treatment, protection of information about oneself as well as one's correspondence, data collection, domestic mirrors and one's good name[47]. This means that no one can be subjected to arbitrary and unlawful interference by another entity. And undoubtedly, the advanced technologies present in our bodies are highly invasive to our overall privacy, if only by allowing

---

[44] Charter of Fundamental Rights of the European Union (2012/C 326/02), Official Journal of the European Union C 326, 26.11.2012.

[45] Convention for the Protection of Human Rights and Fundamental Freedoms, drawn up in Rome on November 4, 1950, European Treaty Series No. 5.

[46] International Covenant on Civil and Political Rights opened for signature in New York on December 19, 1966, Official Journal, 1977, no. 38, item 167.

[47] M. Pryciak, *Prawo do prywatności*, „Studia Erasmiana Wratislaviensia" 2010, t. 4, pp. 211–229.

us to be tracked or analyzing our movements[48]. Already, location privacy is being violated by devices using RFID. Because humans do not feel the transmission used to read data from our chip, RFID tags are ideal targets for eavesdropping. This situation could lead to group profiling, which would be based on the spectrum of data. And this is undoubtedly a manifestation of control, since, properly directed and incentivized, we can make different decisions than we actually want to. As S. Zuboff writes, "automated machine processes not only know our behavior, but also shape our behavior on a large scale"[49]. Socio-economic rights, such as the right to education, may also be threatened, as it may be taken away from those who choose not to have implants that improve their ability to learn.

To sum up, the situation is shaping up in two ways. Namely, cybernetic implants may develop human dignity, by increasing the degree of empathy and compassion towards others. On the other hand, however, which is also more likely, there may be a decrease in authentic, genuine individual-directed actions, leading to a partial or worse overall disappearance of the individual's autonomy, individual subjectivity and, consequently, human dignity.

ICT implants (not) banned by law

At first glance, it appears that ICT implants are unproblematic, especially when it comes to their clinical use. However, analyzing the potential dangers present in non-medical use of the implants, the conclusion arises that the introduction of ICT implants into widespread use may be the wrong move. The lack of precise and binding legislation governing ICT implants gives tacit permission for their misuse. An example of this is the use of ICT implants by untrained adults on children without much, if any, supervision. This situation is a prelude to the exploitation of vulnerable groups for personal gain. Moreover, as research on non-medical applications of

48 *Ochrona prawa do poszanowania życia prywatnego i rodzinnego w Europejskiej konwencji o ochronie praw człowieka*, Rada Europy, Strasburg, 2012.

49 S. Zuboff, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, New York 2019.

implants is just beginning, it is unknown at this point how implants, especially neuroimplants, will affect an individual's functioning. Will it interfere in any way with the consciousness of acts performed, but will this sphere remain unaffected? What if a person with a neuroimplant loses control over his body, and as a result, harms or kills another human being, can this be considered an intentional act and held criminally responsible? Who will be held responsible for this, the entity that carried out the act, or will it nevertheless fall under product liability, or perhaps the doctor who did not sufficiently inform about the risks and uncertainties associated with the implant? The situation raises many questions that for the moment remain without clear and concrete answers.

Looking at the possibility of enriching one's abilities and skills, the natural consequence will be growing pressure among workers to increase their competitiveness in the labor market. This will reflect very negatively on individuals, as they may be more inclined to take risky and dangerous steps, such as inserting untested ICT implants into their bodies, which can harm their health and violate all laws. This in turn leads to the development of a black market, where illegal trade or production of such devices will flourish.

Ambiguities also arise in the context of the democratic rule of law and its possible violations. Admittedly, the European Group on Ethics in Science and New Technologies points out that non-medical ICT implants used for surveillance may only be allowed if the legislature deems it an urgent and legitimate necessity in a democratic society, and there are no less invasive methods[50], but this does not change the fact that widespread and indiscriminate surveillance can occur in this way.

In conclusion, it is impossible to answer unequivocally whether the non-medical use of ICT implants should be prohibited by law or not. Certainly, appropriate regulations are required. In my opinion, however, it is, a very risky action, at least for the moment. Due to, mentioned several times, the lack of a unified as well as codified legal system designed exclusively for non-medical implants, it is very easy for them to be improperly disseminated as well as used. The

[50] EGE 2005, MEMO/05/97.

numerous dangers only intensify doubts about the rightness of the development of the path in question. It is not why individuals have fought and are fighting for autonomy that it should be taken away from them by automated devices. Undoubtedly, this is a significant step in terms of science, however, is the introduction of technology into every aspect of life, including the biological body, worth such a risk? It may bring more losses and problems than benefits. The use of ITC implants for medical purposes is a legitimate need, which as much as possible should continue, because the goal is to correct or improve the quality of life. Non-medical implants are mainly the invention of a consumerist lifestyle focused on making human existence easier, which in the long run may lead to the creation of a generation of helpless beings. Total dependence on technology will result in people not being able to cope with the simplest daily activities when, even if the implant fails. Hence, the introduction of legal restrictions in the context of non-medical use of implants, in my opinion, would be a most appropriate move.

Conclusion

Probably for many people the vision of the development of the idea of transhumanism is still an abstraction, it is, however, slowly becoming a reality. However, analyzing the phenomenon, it is not clear whether the legislation will completely meet all the problems and find adequate solutions, due to the multi-faceted complexity of the issue.

Undoubtedly, the introduction of cybernetic implants into widespread use carries serious ethical as well as legal implications. The whole matter raised requires an interdisciplinary approach to develop a strict, stable and transparent framework for operation.

Although the matter under discussion may arouse extreme emotions, one thing is certain, technological progress still has much to offer us. In the words of Albert Einstein: "If at first the idea is not absurd, then there is no hope for it"[51].

51 *Albert Einstein*, en.wikiquote.org/wiki/Talk:Albert_Einstein [accessed: 12.03.2025].

References

Legal acts

Charter of Fundamental Rights of the European Union (2012/C 326/02), Official Journal of the European Union C 326, 26.11.2012.

Convention for the Protection of Human Rights and Fundamental Freedoms, drawn up in Rome on November 4, 1950, European Treaty Series No. 5.

Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC), Official Journal of the European Communities, L 210, 7.08.1985.

Directive 93/42/EEC of 14 June 1993 concerning medical devices, European Parliament and the Council, Official Journal of the European Communities, L 169, 12.07.1993.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of networks and information systems within the Union, Official Journal of the European Union, L 194, 19.07.2016.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, Official Journal of the European Union, L 321, 17.12.2018.

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL)), Official Journal of the European Union, C 252, 18.07.2018.

International Covenant on Civil and Political Rights opened for signature in New York on December 19, 1966, Official Journal, 1977, no. 38, item 167.

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), Official Journal of the European Union, L 119, 4.05.2016.

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, Official Journal of the European Union, L 117, 5.05.2017.

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, Official Journal of the European Union, L 135, 23.05.2023.

Universal Declaration of Human Rights, adopted on 10 December 1948, France, United Nations Document A/RES/217(III).

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny [Civil Code], Dz.U. [Journal of Laws] 2024, poz. [item] 1061.

Jurisdiction

Wyrok Sądu Najwyższego [Supreme Court Judgment] z 21.03.2007, I CSK 292/06, Legalis nr 156746.

Literature

Albert Einstein, en.wikiquote.org/wiki/Talk:Albert_Einstein [accessed: 12.03.2025].

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012.

Bączyk-Rozwadowska K., *Odpowiedzialność cywilna za szkody wyrządzone w związku z zastosowaniem sztucznej inteligencji w medycynie*, „Przegląd Prawa Medycznego" 2021, t. 3–4, pp. 45–60.

Birnbaum Z.P., *Regulating the cyberpunk reality: private body modification and the dangers of 'body hacking'*, „Journal of Business & Technology Law" 2021, vol. 16, issue 1, pp. 119–145.

Bockman C.R., *Cybernetic-enhancement technology and the future of disability law*, „Iowa Law Review" 2010, vol. 95, no. 4, pp. 1315–1346.

Curley B., *Hackers can access pacemakers, but don't panic just yet*, 13.04.2019, foxnews.com/health/hackers-can-access-pacemakers-but-dont-panic-just-yet [accessed: 12.03.2025].

Ethical aspects of ICT implants in the human body: opinion presented to the Commission by the European Group on Ethics, MEMO/05/97, Brussels, 17.03.2005.

Gasson M.N., Koops B.J., *Attacking human implants: a new generation of cybercrime*, „Law, Innovation and Technology" 2013, vol. 5, issue 2, pp. 248–277.

Gruchoła M., *Wartość ciała biologicznego i ciała humanoida w świetle założeń teologii ciała*, „Kultura Słowian. Rocznik Komisji Kultury Słowian PAU" 2023, t. 19, pp. 215–227.

Halamka J.D., Juels A., Stubblefield A., Westhues J., *The security implications of VeriChip cloning*, „Journal of the American Medical Informatics Association" 2006, vol. 13, no. 6, pp. 601–607.

Hines N., *Neural implants could let hackers hijack your brain*, 6.08.2016, inverse.com/article/19148-neural-implants-could-let-hackers-hijack-your-brain [accessed: 12.03.2025].

Human ICT implants: technical, legal and ethical considerations, eds M.N. Gasson, E. Kosta, D. Bowman, Hague 2012.

Klichowski M., *Edukacja cyborgów. Jak działać, by nowe technologie były sprzymierzeńcem a nie wrogiem?*, Poznań 2015.

Księżak P., *Prawo cyborgów (2). Własność i dobra osobiste*, „Głos Prawa. Przegląd Prawniczy Allerhanda" 2022, t. 5, nr 1(9), poz. 12, pp. 45–60.

Nierengarten M.B., *Protecting medical devices against cyberthreats*, 24.09.2017, enttoday.org/article/protecting-medical-devices-cyberthreats [accessed: 12.03.2025].

Organs, European Commission, health.ec.europa.eu/blood-tissues-cells-and-organs/organs [accessed: 12.03.2025].

Perakslis C., Michael K., *Ethical issues to consider for microchip implants in humans*, „Ethics in Biology, Engineering and Medicine: An International Journal" 2012, vol. 3, no. 1–3, pp. 75–86.

Perry P., *Scientists discover how to implant false memories*, 15.06.2016, bigthink.com/surprising-science/scientists-have-discovered-how-to-implant-false-memo [accessed: 12.03.2025].

Popović M.B., *Biomechanics and robotics*, New York 2013.

Pryciak M., *Prawo do prywatności*, „Studia Erasmiana Wratislaviensia" 2010, t. 4, pp. 211–229.

Quigley M., Ayihongbe S., *Everyday cyborgs: on integrated persons and integrated goods*, „Medical Law Review" 2018, vol. 26, issue 2, pp. 276–308.

Singh S., *Transhumanism and the future of humanity: 7 ways the world will change by 2030*, 20.11.2017, forbes.com/sites/sarwantsingh/2017/11/20/transhumanism-and-the-future-of-humanity-seven-ways-the-world-will-change-by-2030 [accessed: 12.03.2025].

Uberveillance and the social implications of microchip implants: emerging technologies, eds M.G. Michael, K. Michael, Hershey 2013.

Warso Z., Gaskell S., *Sienna D3.2: analysis of the legal and human rights requirements for Human Enhancement Technologies in and outside the EU* [WP3 – Human enhancement: ethical, legal and social analysis], 2019, https://doi.org/10.5281/zenodo.4066616.

Warwick K., Gasson M.N., *Practical experimentation with human implants*, [in:] *Uberveillance and the social implications of microchip implants: emerging technologies*, eds M.G. Michael, K. Michael, Hershey 2013, pp. 69–84.

What is hacking, kaspersky.com/resource-center/definitions/what-is-hacking [accessed: 12.03.2025].

Zuboff S., *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, New York 2019.

Abstract
Cybernetic implants in non-medical applications. Selected aspects

The purpose of this article is to present the path of development of implants, once used exclusively for medical purposes and now widespread in non-medical aspects. The inadequacy of previous efforts to combat health problems has forced the search for new, more effective methods, and these have emerged with the development of technology. As a result, implants were created using the existing correlation between computing and communication, which at the same time initiated research into devices inserted into the body to enrich its capabilities. This, in turn, raises a number of difficulties on various levels of life, so an analysis of possible potential risks has been made. Undoubtedly, it is obligatory to implement a number of changes in relation to the new solutions. An attempt was also made to answer the question of whether the non-medical use of ITC implants should be prohibited by law?
Key words: technology, communication, implants ICT, threats, law, medical implants, non-medical implants