# WEARABLES IN THE CONTEXT OF THE RIGHT TO PRIVACY AND DATA PROTECTION – RESEARCH RESULTS AND CONCLUSIONS

Natalia Kalinowska / Katarzyna Morawska

Natalia Kalinowska, lawyer, PhD student, Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration
Wóycickiego 1/3, 01-938 Warszawa, PL
nm.kalinowska@gmail.com; www.uksw.edu.pl

Katarzyna Morawska, lawyer, PhD student, Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration
Wóycickiego 1/3, 01-938 Warszawa, PL
morawskatarzyna@gmail.com; www.uksw.edu.pl

***Keywords:*** ***Data concerning health, GDPR, personal data protection, wearables***

***Abstract:*** *Smart Watches, Smart Bracelets and Smart Glasses belong to the group of equipment so-called wearables, which are becoming more and more popular each year. These devices are especially popular with athletes, businessmen and people interested in new technologies, and thanks to the constant monitoring of vital functions – more and more often by chronically ill people. It is believed that wearables will revolutionize the treatment system and give new possibilities for the analysis of medical data. Despite of the benefits of using medical data collected by wearables, there are a lot of negative aspects relating to processing that data. Taking into consideration that the use of wearables is a novelty and taking on the insufficient amount of research on the relationship between the implementation of the provisions of the GDPR, and protecting the privacy of users of wearables, it was decided to carry out surveys. The aim of the research was to determine the state of awareness of users using wearable devices both in terms of benefits and threats, related to the processing of health data by these devices.*

## 1. Introduction

Nowadays wearable devices are one of the most important aspects of every discussion related to the Internet of Things (IoT). The sale of wearable devices is increasing year by year. The wearable market is expected to jump from an estimate of 16 billion dollars in 2016 to over 73 billion in 2020.[1] Wearable devices are very popular, especially in the health sector, because it is often believed that they will revolutionize the treatment system and give new possibilities for the analysis of medical data.

Despite of undoubtedly numerous benefits of using medical data collected by wearable devices, it should be also outlined that using wearables could lead to negative consequences relating to the processing of personal data[2]. This issue has become the reason to conduct a research to determine the state of awareness of users both in terms of benefits and threats related to the processing of health data by these devices.

Because wearables are still not that common in Poland, the presented results are focusing on the basic and most important issues surrounding the right to privacy while using wearables.

---

1 Wearable device sales revenue worldwide from 2016 to 2022 (in billion U.S. dollars), source: https://www.statista.com/statistics/610447/wearable-device-revenue-worldwide/, (all websites last accessed 6 January 19).

2 Genaro Motti V. / Caine K., *Users' Privacy Concerns About Wearables*, source: https://www.researchgate.net/publication/300475609_Users'_Privacy_Concerns_About_Wearables, George Mason University 2015; see also: Threats and inconveniences arising from the use of IoT according to Polish users, from report by AIB Polska, Report on Internet of Things in Poland, source: https://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf.

The main aim of this article is to present the benefits and threats for the individual and society (related to the use of such devices in the health sector), the results of research on the level of awareness of wearable devices users, to determine the current legal regulation and to verify whether it is necessary to take legislative action in this area.

## 2. Benefits and threats connected with processing health data by wearables

Using wearables has many advantages, especially for the health sector, which thanks to the amount and accuracy of data processed by these devices can significantly improve the treatment and diagnosis of patients. That information can be used to accelerate the time of treatment, and reduce costs for the patient and for the state, especially in health services. Smart usage of the data collected by wearables can have a preventive function by minimizing the possibility of wrong diagnosis and side effects caused by it. Collected data can also help to prevent the development of chronic diseases.

Because wearables can monitor health condition in many ways the conclusions obtained on the basis of the collected data can be very broad. For example, that information may be very helpful for doctors to respond properly in case of a drastic change in patient's health condition. The possibility of easy access to data about the patient and constant monitoring can also reduce the need for permanent personal care (doctors and relatives).

Diagnosis can be faster and cheaper and these factors can help to increase the level of patient services. The more information the doctors will have access to, the more chances to minimize risks for errors in medical assessment. Moreover, shortened time for diagnosis can help to increase the amount of examined patients. The treatment can also be cheaper so more patients will be able to take advantage of it. From the general perspective, providers of wearables can predict and thus eliminate the occurrence of an epidemic. However, wearables can also be treated as a potential big threat to the privacy of the individuals.

Regarding negative consequences, the vast social impact that wearables can have should be pointed out. Collected data means excessive knowledge about medical conditions that can be used in various cases and by banks, insurance companies, or employers. Moreover, this can cause dismissal, increases in insurance premiums, lack of possibilities to get a loan, social ostracism and exclusion from healthcare services. It is also important to outline that service provider can collect data which can be excessive in accordance with the purposes of processing the data, such as additional geolocation data, behavioral data.

Due to lack of awareness about the consequences, some people agree to permanent surveillance without having read the terms of use. This leads to risks related to data protection, especially when it comes to proper security measures (high risk of hacking the system) and knowledge about the rights of data subject.

## 3. Wearables in the context of legal regulation

Wearables, as part of a huge group of phenomena (generally called the IoT), raise many ethical and legal issues. These challenges relate, among other things, to the fact that the IoT analyses the collected data (for example from wearables) and makes inferences about human behavior or health problems. To do this, the IoT, including wearables, uses solutions that include artificial intelligence (AI), which replaces the limited capabilities of the human being in processing huge amounts of collected information.

Discussing wearables in legal or ethical aspects, these considerations should be started by defining the concept of AI. To do so, we will use the proposed definition from the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions called «Artificial Intelligence for Europe» that says «AI refers to systems

that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals».[3]

In the context of legal challenges, especially taking into consideration the subject of the survey, which was carried out for the purposes of this publication, attention should first be paid to issues related to the protection of human rights, personal data and consumer rights.

Among the specific issues highlighted by the Ministry of Digitization in Poland in the report «Assumptions for AI strategy in Poland»[4], which was prepared along with experts in the field of new technologies, it is indicated that all legislative changes should aim at greater enforceability and data security, and should also consist of transparency in all processes that take place in connection with the use of AI. These conclusions formulated for the needs of AI can be referred directly to the IoT area.

Taking into consideration the outcome from the Ministry's report the issue of the IoT and AI is connected with the necessity to develop a comprehensive, interdisciplinary approach that requires constant amendments in almost every area of law. Therefore, it is impossible to assess, for the purposes of this article, all legal acts currently in force that address issues pertaining to the IoT, in particular in the context of wearables in healthcare. In the publication it will present the directions for changes, which primarily pay attention to building awareness and transparency of the process.

In the context of building greater awareness among users, it is pointed out the need to ensure transparency at the legislative level regarding the actions performed by devices and the type of algorithms they use, the rules of informing users how to check or correct decisions taken by AI. This issue is particularly vital to understand how those devices work and what is the basis on which decisions are being made. Considering that 25% of the respondents to the question «Would you consent to providing health information that has been obtained by devices such as smartwatches, in exchange for lowering the loan installment / insurance premiums?» answered «yes» and 25% users indicated that «it depends on the amount of the discount», this postulate seems particularly important.

IoT involves processing huge amount of personal data in an environment exposed to a high risk of losing security of this data and thus the risk of losing confidentiality. Therefore, the personal data controllers should comply with the obligations set out in the GDPR[5] in a particular scrupulous manner. And in this case, the regulations already indicate the obligation to maintain transparency while processing the data and their scope. That is connected to the obligation to provide data subjects with the information obligation while maintaining all the requirements set out in Articles 12, 13 and 14 GDPR. Consequently, the GDPR indicates the obligation for controllers to process personal data in right purposes and on proper legal basis, determining the period of data storage. Apart from the above, controllers have much more responsibilities that are designed to protect privacy such as data protection by design and by default set out in article 25 or data protection impact assessment (art. 35 GDPR).

While considering data privacy it should be outlined the forthcoming ePrivacy Regulation (ePR)[6] that will be a regulation comprehensive to GDPR and will affect IoT devices strongly, since it will apply only to electronic communications. The European Parliament underlines that the confidentiality of electronic communications

---

3 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, 25 April 2018, COM(2018) 237 final, Brussels.

4 Ministry of Digitization in Poland, «Assumptions for AI strategy in Poland», 9 November 2018, Warsaw.

5 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 (GDPR), published in the Official Journal of the European Union L 119, p 1.

6 Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

requires even higher protection than the one settled by the GDPR and that consent from end-users should be obtained systematically[7].

Among the challenges in the field of civil law, attention should be paid to the issues concerning legal personality of AI. There are still discussions as to whether AI should and if so, to what extent obtain legal personality. In the Ministry's report experts were clearly opposed to such solution due to the difficulties in pursuing claims for damages. Consumer regulations will also have to be changed, in particular in terms of information obligations created by entrepreneurs. There is a need to create legal mechanisms that guarantee the consumer full and real information about the scope, mechanisms or entities using data about the consumer.

## 4. Conclusions for the research

The survey was carried out on a group of 1029 people from Poland during a period of two weeks. That was a preliminary research, therefore the scope of demographic variables was limited to gender, age and education level. The aim of the study was to verify the relationship between the intensity of use of wearable devices and awareness of data processing, concerns about the use of wearable devices, knowledge about the possibility of modification of processed data and awareness of the purpose, methods and scope of processed data.

The study confirmed that wearables are still new on the technology market, and, in contrast to smartphones, they are a gadget rather than a device we cannot live without[8]. While the use of smartphones is highest in the age group 18–24, the use of wearables is highest in the group of respondents aged 35 to 44 and 45 to 54 (47% of respondents in both age groups indicated the use of wearable devices).

| Results in particular groups: | **Do you use wearables?** | |
|---|---|---|
| **Age** | **Yes** | **No** |
| younger than 12 | 0% | 100% |
| 13-18 | 20% | 80% |
| 19-24 | 18% | 82% |
| 25-34 | 32% | 68% |
| 35-44 | 47% | 53% |
| 45-54 | 47% | 53% |
| 55-64 | 20% | 80% |
| 65 and older | 0% | 100% |
| **Results in total:** | **31%** | **69%** |

**Table 1. The relationship between the age of respondents and the use of wearables**

The highest number of respondents using wearables has higher education (78,5%).

[7] Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, source: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_on_eprivacy_en.pdf.

[8] According to CBOS research, the use of mobile phones every year increasingly displaces the use of landline telephones. Currently, 97% of Poles use mobile phones, and 57% of them have a smartphone, source: https://www.cbos.pl/SPISKOM.POL/2017/K_099_17.PDF.

| **Users of wearables and the level of education** | |
|---|---|
| None – I'm still learning | 3,74% |
| Basic education | 0% |
| Secondary education | 17,76% |
| Higher education | 78,50% |

**Table 2. The level of education of respondents who use wearables**

On the other hand, when comparing the results with people with the same level of education, the highest level – 34%, was in the group of people with the secondary education.

| | **Do you use wearables?** | |
|---|---|---|
| **Level of education** | **Yes** | **No** |
| None – I'm still learning | 29% | 71% |
| Basic education | 0% | 100% |
| Secondary education | 34% | 66% |
| Higher education | 31% | 69% |

**Table 3. The relationship between the level of education of respondents and the use of wearables**

The research has shown that only 31% of all respondents use wearables. It is possible that the reason for this situation is (*inter alia*) the high price of these devices – only 21% of respondents indicated that price is an advantage).

Such respondents, who are the users of wearables appreciate ease of use, functionality, availability and variety of products on the market. The table below presents the main purposes of using wearables (respondents could mark more than one answer). Respondents mostly use wearables for monitoring daily activities and while excercising. A lot of people also use it for monitoring their sleep. This result shows the scale of use of these devices, including the scale of health data.

| Purpose of using wearables | Percent of respondents |
|---|---|
| monitoring daily activities (eg number of steps, heart rate) | 87% |
| sleep monitoring | 39% |
| while doing exercises (eg while running) | 56% |
| checking the date and time | 78% |
| receiving calls | 37% |
| replying to messages | 30% |
| making payments | 12% |
| none of the above | 2% |

**Table 4. Reasons for using wearables**

Unfortunately, respondents do not pay much attention to the security of their data. Most of the respondents who use wearables to monitor daily activities have only partial knowledge of what data the device collects about them, but only 22% of respondents declare that they have full knowledge in this field.

| People who have marked the following goals: | Do you know what data the device collects about you? | | |
|---|---|---|---|
| | Yes, to the full extent | Yes, but only partially | No |
| monitoring daily activities (eg number of steps, heart rate) | 22% | 66% | 12% |
| sleep monitoring | 29% | 64% | 7% |
| while doing exercises (eg while running) | 25% | 63% | 12% |

**Table 5. The relationship between the ways of using wearables and the knowledge of the data that device processes**

Although 66% of respondents read the information clause, every third respondent declared that he had a problem finding it and it required him to take action to find this information.

| People who have marked the following goals: | Have you read the information about the processing of personal data? | | |
|---|---|---|---|
| | Yes | Yes, but it was not visible immediately and you had to look for by yourself (e.g. go to the website of the producer) | No |
| monitoring daily activities (e.g. number of steps, heart rate) | 44% | 22% | 34% |
| sleep monitoring | 52% | 24% | 24% |
| while doing exercises (e.g. while running) | 47% | 22% | 31% |

**Table 6. The relationship between the ways of using wearables and reading the information about data processing**

On the other hand, users take active steps to adjust the amount of information that the device collects about them. This particularly applies to those who have declared to read the information clause and who have read the clause after difficulties in finding it. The research clearly showed that reading the information clause had a direct impact on changing the scope of information collected by the device.

| | Have you changed the default settings to adjust the amount of information that is processed (collected and analyzed) by the device? | | |
|---|---|---|---|
| | | Yes | No |
| Have you read the information about the processing of personal data? | Yes | 87% | 13% |
| | Yes, but it was not visible immediately and you had to look for by yourself (e.g. go to the website of the producer) | 62% | 38% |
| | No | 45% | 55% |

**Table 7. The relationship between people who have read the information about data processing and the tendency to change the default settings of the device**

Respondents are largely aware of the risks associated with the use of wearables. 68% believe that their data can be used by unauthorized entities. 59% indicate as a disadvantage that devices can collect data in a much wider range than necessary for the service provided, 45% of them share the opinion that there is a risk of data being stolen and 43% as minus of wearables indicates the possibility of creating profiles based on their personal data.

## 5. Summary

The results show that people are aware mostly at the general level about the processing of their data by these devices. Those of them who have read the information clause take active and conscious actions to protect their privacy. Most of them are convinced that their knowledge is not complete. Despite appreciating the functionality of ease of use or the variety of products offered on the market, they also know the possible threats connected with using them e.g. unauthorized access to data, creating profiles on the basis of collected data or collecting too much data. Those doubts may, *inter alia*, explain why only 31 % of the respondents are using wearables.

Unfortunately, despite the high level of awareness regarding data security threats, there is still a need to educate about the actions to be taken in the event of a breach of data security. It is to be hoped that the provisions of GDPR implemented in May 2018, obliging controllers (in case of a data breach) to notify the data subject, will help raise the level of knowledge in this area. The research has also shown the willingness of respondents (25% of them) to agree to the processing of their health data in exchange for the possibility of obtaining, for example, a lower insurance premium. This shows lack of awareness of the importance of such data and possible negative consequences for the person who agrees.

Nowadays, in the era of information society, the role of public authorities is particularly important. They should, through responsible and thought-out legislative activities, regulate the processing of personal data, especially health data (as specific category data).

The actions of the Polish government in the field of attempts to regulate issues related to AI should be positively evaluated. Also, at the level of the European Union, activities on legal regulations in the field of AI have been initiated[9].

Undoubtedly, a comprehensive approach to the processing of personal data regarding the health condition of such devices is necessary, because despite the many benefits associated with their use, the inaccurate use of this data can cause far-reaching consequences for their users.

Finally, it is worth recalling the famous phrase spoken by prof. Elżbieta Traple «*The law will never catch up with new technologies*».[10] For this reason, we should increase the awareness of users about the risks associated with their use of wearables, but first of all taking social actions to encourage people to modify the amount of data collected by the device and show who should they contact with in the event of a data breach.

[9] https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

[10] S. Wikariak, Prawnicy nigdy nie dogonią postępu technicznego, source: https://prawo.gazetaprawna.pl/artykuly/868479,prawnicy-nigdy-nie-dogonia-postepu-technicznego.html.