Legal Issues in the Digital Age. 2024. Vol. 5. No. 3.
Вопросы права в цифровую эпоху. 2024. Том 5. № 3.

IT, Industries, Law

Research paper
УДК: 342
JEL: K2
DOI:10.17323/2713-2749.2024.3.49.67

Legal Regulation of Smart Wearable Devices in China

Li Yao
Institute for Foreign-Related Rule of Law, East China University of Political Science and Law, 555 Longyuan Str., Area Songjiang, Shanghai, 201620, China, yaozaihenmang@mail.ru, ORCID 0000-0002-9933-7513

Abstract

A smart wearable device is a portable intelligent gadget worn directly on the body or integrated into clothes or accessories that along with other features such as portability, mobility, sustainability, interactivity and ease of control exploits the natural ability of human body or environment to exchange information with the user, monitor human health and provide entertainment via built-in sensors, wi-fi communication, multimedia technologies, integrated microchips, etc. There are diverse smart wearable devices such as watches, bracelets, massage tools of various types etc., with usage scenarios ranging from general business uses to professional medicine and health care. High demand and technological progress are boosting the market for smart wearable devices that becomes increasingly attractive. Notably, smart wearable devices are not only hardware but also powerful functionalities supported by applications and cloud computing that collect and generate large amounts of operating data, only to cause widespread concern due to the underlying privacy and data security issues. The paper explores how wearable devices collect data and what risks are involved while providing an overview of the applicable regulation in China and explaining the existing gaps (such as the term "consent" to be clarified in the effective law) and personal data anonymization problem, proposing advice for better regulation as well as the ways to specify the provisions for informed consent, dynamic assessment of anonymized data, etc.

Keywords

smart wearable devices; risk; privacy; personal data anonymization; consent; Chinese law.

For citation: Li Yao (2024) Legal Regulation of Smart Wearable Devices in China. *Legal Issues in the Digital Age,* vol. 5, no. 3, pp. 49–67. DOI:10.17323/2713-2749.2024.3.49.67

Background

Rapid progress of the Internet of things, AI, big data and other next generation data technologies have opened up unprecedented opportunities for the development of wearable devices ranging from the early simple pace-counters to today's multi-functional watches for health and fitness monitoring, mobile payments etc., and up to such devices as smart clothes and AR/VR glasses and headsets. Thus, on 5 June 2023 Apple presented the Vision Pro headset at the WWDC which, compared to the existing VR glasses, integrates the AR (Augmented Reality) technology activated by a lever in the upper part of the headset which, based on the Apple Watch operating system logic and the proprietary spatial computing technology, allows users to see floating virtual interfaces in their real environment. As a fantastic feature, multiple built-in sensors make Vision Pro sensitive to movements of the user's eyes and hands for easy control of the virtual interface with eyes, gesture and voice without joystick or other interactive device. VR devices exemplified by Vision Pro are crucial for access to the metaverse, with numerous types of these devices such as VR glasses, VR helmets and digital VR gloves already available. On 23 April 2024, Meta, a specialist in virtual reality and metaverse, announced the launch of the Meta Horizon OS quest system, with Asus and Lenovo already under contract with Meta for forthcoming production of MR headsets based on Meta Horizon OS. For more natural user experience, Meta Horizon OS integrates numerous self-monitors and other technologies for four new types of communication including hands, eyes, face and body monitoring. While Meta's previous Quest platform had control regimes based on the use of joystick or buttons, new Meta headsets for multi-modal AI control support based on numerous key technologies for 3D simulation, rendering, man-machine engagement, high resolution displays, AR capabilities and

virtual avatars will continue to offer breathtaking and interactive virtual reality experience in a limited environment. With Google 2024 I/O annual conference taking place as planned on 14 May 2024, a number of new AI functions and forthcoming products including Google's own Project Astra multi-modal AI assistant combined with AR glasses promotional videos were announced. Project Astra is expected to memorize and analyze what it sees in addition to audio, text and visual data processing capabilities typical of conventional multi-modal AI macro-models. Wearable devices have largely improved daily life. To encourage further development of the industry, China has implemented the relevant policies for rapid growth of wearable devices in medicine, health care and consumer goods sectors. Meanwhile, there is an expansion of smart wearable devices relying on man-machine engagement and user behavior-related big data that record physiological conditions and behavioral path on a permanent basis thus inevitably creating specific risks to be addressed by law.

1. China's policies in respect of smart wearable devices

A large-scale electronic industry in China is the result of many years of development, with smart wearable devices forming a mature segment of important intelligent products. Boosted by the increasing domestic and international demand and more sophisticated technologies, all types of electronic products have been improved in terms of their design, quality, performance and other aspects, only to encourage domestic producers of wearable devices to further upgrade R&D, production and branding, with competent public authorities introducing a number of measures in recent years.

In June 2016, the State Council published the Framework of the 2030 Healthy China Action Plan: "Developing and promoting digital intelligent devices for health care. Supporting health-related AI research and development, 3D biological printing technologies, medical robots, large medical equipment, auxiliary devices for health and rehabilitation, smart wearable devices and the relevant micro-sensor devices"[1].

In February 2022, the State Council published the 14th five-year plan for development of the anti-ageing national program and pension security

[1] Available at: https://www.gov.cn/zhengce/2016-10/25/content_5124174.htm?eqid=9d4da6bb000833c0000000046496f297 (accessed: 15.06.2024)

stressing demand for "rehabilitation treatment of neurological disorders, post-traumatic cognitive brain disorders, support for people in paralysis, revolutionary brain-computer interface and other technologies, assistive robots for rehabilitative support for various injuries, and implementation of the action plan for development of intelligent service robots, R&D of wearable dynamic devices for ECG monitoring and other equipment for physiological parameter testing, portable health monitoring equipment, self-service and other health monitoring tools, as well as development of new types of microchips for signal recording and intelligent digital health terminals"[2].

In April 2023, the Ministry of Industry and Information Technology issued a circular to support joint innovations and 5G+ Smart Tourism development: "Encouraging the development of 5G applications based on the smart tourism information platform, promoting in-depth integration of digital products such as 5G cameras with embedded AI, VR/AR terminals and smart wearable devices with intelligent tourism products, as well as further promoting 5G intelligent tourism products"[3].

In July 2023, the State Council issued the Notice on consumption recovery and support measures: "Encouraging the consumption of smart wearable devices and intelligent products, as well as develop new usage scenarios for electronic products"[4].

In January 2024, the State Council issued the Opinion on promoting Silver Hair Economy and improving the well-being of elderly individuals: "Improving the list of intelligent products for healthy ageing, promoting a new generation of information technologies and mobile terminals, smart wearable devices, service robots and other intelligent devices for homes, communities, institutions and other settings, developing smart products for health management, care and psychological comfort of the elderly"[5].

As follows from the above national policies, thanks to breakthrough achievements in such innovative areas as AI, data storage and computing,

[2] Available at: https://www.gov.cn/zhengce/zhengceku/2022-02/21/content_5674844.htm (accessed: 15.06.2024)

[3] Available at: https://www.gov.cn/zhengce/zhengceku/2023-04/12/content_5751000.htm (accessed: 16.06.2024)

[4] Available at: https://www.gov.cn/zhengce/content/202307/content_6895599.htm (accessed: 17.06.2024)

[5] Available at: https://www.gov.cn/zhengce/zhengceku/202401/content_6926088.htm (accessed: 17.06.2024)

brain-computer engagement technologies, and promoting the metaverse concept, the usage scenarios of smart wearable devices, ever wider and diverse, will apply not only to gaming, entertainment and tourism but also health management, intelligent medical services, sports and fitness, smart furniture and care for the elderly, and to the development of intelligent, individual and traceable user services.

2. Data collected by smart wearable devices and relevant risks

Broader usage and convenience of smart wearable devices comes at a cost of permanent "surveillance" of users by these devices. Shaped by the information age, smart wearable devices carry cameras, sensors, chips and other sophisticated equipment sensitive to physiological conditions of human body and able to collect real-time data and engage with a cloud or software for personalized reporting, only to make the underlying usage scenarios highly sensitive to personal data collection as manifested by the following:

Firstly, automatic real-time collection of data. In traditional devices, information is normally collected partially and in a fragmented way while smart wearable devices are capable of continuous collection of data that can follow changes to the human health in real time. The man-computer engagement logic is that the line between man and machine, body and environment gradually fades. In mobile scenarios, wearable devices are linked to human body thus connecting people, behaviors, scenarios and networks, with the body and media mixed together, reality and virtuality mapping over each other, so that human biometric data, information on health, fitness, geographic position and environment is monitored round the clock. Surveillance permeates our daily life like air and water. As has been noted in literature, "thanks to round-the-clock following, monitoring, reminding and feedback, smart wearable devices, like smart companions, become a kind of replacement for human limbs, a technological shadow body where the subject is digitally assembled from different behavioral patterns to become a walking digital man embedded, every time he opens his eyes, into a heterogeneous environment of multidimensional time that is real and virtual, private and public" [Xu T., 2022: 163].

Secondly, pervasiveness. A smart shadow companion, the wearable device not only collects static biometric information such as cardiac rate, myo-electricity, pulse, blood pressure, oxygenation, body temperature etc.,

but also assesses and recognizes the user's behavior and state (whether he sits or stands, runs or jumps, works or sleeps, walks or falls), location and environment (weather conditions, barometric pressure, altitude) and other related data. In short, the wearable device can present a full picture of human health and daily activities by generating the user's exact profile. Types of data collected by wearable devices embrace virtually all human states over the day: at work, a smart watch will remind users: "please take a walk, do not sit still"; during physical exercising, "steps, cardiac rate, blood oxygenation, arterial tension, palpitation"; during sleep — state and time of sleep. Relying on novel technologies, VR products can not only collect users' external biometric data such as iris diaphragm, fingerprints, body height, constitutional type, voiceprints etc., but also physiological information by monitoring heartbeat and muscular response. The progress of the brain-computer interface has resulted in mind control, only to mean that the data detection "pinhole" can go deep "under the skin" and assess human brain data such as thinking, consciousness and memory, one by one. BrainLink, a smart headband developed in China, is advertised to monitor the user's brain, for example, whether it is tense, relaxed or tired [Wei Z., Shi H., Cao T., 2020: 19]. Once illegally transferred and sold, such data can be applied in many ways, not only violating the right to privacy but also creating major social problems such as discrimination at employment, thus adding up to the dilemma of science and technology ethics.

Thirdly, more parties involved in the process. Wearable devices have more segments of information flow including data collection, storage, use exchange, provision and deletion which may involve consumers, patients such as elderly people and children, service providers, health institutions, governments and other multilateral subjects, with a higher risk of leakage and unauthorized processing. In contrast, traditional health care assumes a process focused on in-patient consultations with lower-risk circulation of information within the hospital. Meanwhile, proprietary technologies of wearable medical devices are focused on digital data processing and transfer via wireless communications including diffraction bio-signals, navigation, cloud storage, fingerprint identification, data requests, fees, filming, screening, AI, medical visualization, nanoinjections, connectivity, resource and energy distribution, etc. [Liu X., 2020: 39-41].

Fourthly, multiple use. When marketed, Apple Watch was advertised as "saving lives ruined by mobile phones" while it would penetrate inside the body under the pretext of "exercising for health" [Song M., Xu S., 2020:

47]. While users assess and monitor the state of their health and regulate physical exertion through the use of wearable devices posting the results to social platforms in real time, it feels as if they were filmed by a security camera. The use of personal data in wearable devices has gone well beyond simple health monitoring to serve secondary purposes. If we integrate and process the information collected by wearable devices, we will get indirect data of substantial informative value. For example, body data collected by these devices can be professionally analyzed to generate user health reports, with a back office to tell on this evidence whether the user has suffered or will suffer from certain disease; credit or insurance companies to charge higher premiums or even assess the feasibility of insurance services in view of the reported state of health. Correlation analysis of cardiac rate, oxygenation, deep sleep and other data can help to detect whether the user suffers from cardiovascular diseases while businesses can use these data to offer certain medical goods and drugs. As another example, the extent of papillary dilatation can reveal a preference for something, and eye-tracking technology can tell whether the user has recognized something by the movement of his eyes; if we link this data with the user's location or address, we can recommend a fitness center, restaurant or other recreational site. Using personal data brings enormous potential to businesses leading to re-use of personal data. At this moment, "the user becomes a link in production chain where he will permanently generate both data and feedback on data usage" [Hu L., 2018: 91].

The growing use of wearable devices and supporting applications is fraught with three main threats related to the extent and sensitivity of data being collected: privacy, data use and exchange, and also the risk of hacking.

Firstly, a new type of privacy risk. Smart wearable devices collect real-time data on pulse, blood pressure, respiratory rate, sleep, physical exertion, dietary preferences, lifestyle etc., while health data are currently the most confidential type of information. While users voluntarily collect and analyze the said data via wearable devices to generate personalized reports, they might be unaware that these devices can collect their other data along the way. Moreover, with technological change smart wearable devices are able to make and accept calls, send and receive messages, make instant payments meaning that the wearable device should have real-time connectivity to the user's smartphone, with supporting mobile applications constantly collecting different data from the smartphone in the background. While all data collected by smart wearable devices are accessible to their manufacturers, the user collecting the data is unaware what information

is collected. This results in information asymmetry and round-the-clock privacy threat to the user.

Secondly, risks of unauthorized data use: what the collected data will be used for and whether they will be made available to third parties. In the age of big data, data are as valuable as oil, and it is only natural that smart wearable devices in contact with the user round the clock 7 days a week will use this advantage. Many companies share the collected data with the third parties to maximize their profits. Thus, consumption data are sold to advertisers for better targeted advertising while physiological data and those on habits for physical exertion can be made available to insurers for higher premiums. Since firms increasingly use consumer data in new and different ways, it may result in a loss of control over users' personal data when wearable device manufacturers and their partners will know more about users than users themselves. With more data transferred and used, the leakage risk is higher. Where personal data are transferred and processed by several entities, users will find it hard to understand where their data go and why they are processed, only to create a "black box effect".

Thirdly, risks of hacking. Under the current design and development pattern, the focus is on higher performance and lower weight of wearable devices, with a majority of manufacturers unaware of security issues and even willing to compromise for the sake of performance thus increasing the risk of hacking. While the data collected by smart wearable devices are normally not encoded, abusers can have access to user personal data and location via the Bluetooth connectivity to monitor user actions and even remotely control the devices, only to threaten the security of persons and property. Some studies have demonstrated that personal health data is information on someone's physical or psychic health received in process of preventive care, diagnostics, treatment etc. It is a symbol related to a particular person reflecting individual traits and enabling identification [Tian Y., Zhang Y., 2021: 50]. In 2022, 41 percent of advanced persistent threats (APT) will be related with the government and health care, with attacks on health care to account for 15 percent of total APT attacks in China, second only to the government sector[6]. Malware or application errors can equally result in unauthorized access to data saved in wearable devices, with design errors at the top of statistics of vulnerability causes[7].

[6] Available at: https://www.qianxin.com/threat/re-portdetail?report_id=151 (accessed: 17.06.2024)

[7] Available at: https://www.topsec.com.cn/uploads/2024-01-04/5573280d-c531-4b57-8407-deaa347472e91704359364603.pdf. (accessed: 18.06.2024)

3. China's regulatory framework and gaps

3.1. Legal regulation overview

At this stage, China's personal data protection law mainly splits into two parts: private and public law.

As to civil law, personal data protection in China is largely governed by the Civil Code of the People's Republic of China (hereinafter Civil Code of China) and by the Law on Personal Data Protection. The Civil Code of China explicitly considers biometric information as personal data in the "personal rights" section protectable together with the right to privacy, with relevant legal remedies available to civil law subjects[8]. The Law on Personal Data Protection provides for persons' right to informed consent to personal data processing that could be withdrawn, and for processing agents' duties to classify and manage personal data[9].

From the perspective of the Criminal Code of the People's Republic of China (hereinafter Criminal Code of China), the main crimes related to personal data security[10] are offenses against personal data of individuals (Article 253.1) while the Supreme Court and Procurator General Office in their Explanation on applying legal provisions to personal data-related criminal offenses have stated: "Illegal ownership, sale or presentation of personal data shall be deemed an aggravating circumstance envisaged by Article 253.1 of the Criminal Code of China where it has occurred in one of the following situations:... 4) illegal ownership, sale or presentation of over 500 personal data units such as information on housing, communication records, physiological and health data, transactional and other data likely to impact the security of persons or property"[11]. Other offenses are related in the Criminal Code to illegal penetration and destruction of computer systems (Article 285); non-compliance with data security duties (Article 286.1); and illegal use of data networks (Article 287.1).

---

[8] Available at: https://www.gov.cn/xinwen/2020-06/01/content_5516649.htm (accessed: 18.06.2024)

[9] Available at: https://www.jxrtvu.com/xdjyjszx2023/2022/0906/c3642a29877/page.htm (accessed: 19.06.2024)

[10] Available at: http://www.law-lib.com/law/law_view.asp?id=768114&page=2 (accessed: 19.06.2024)

[11] Available at: https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml(accessed: 19.06.2024)

As to administrative law, China's legislative framework on personal data security is scattered across a variety of regulations, standards etc. For example, the Data Security Technology Specifications for Personal Data Protection (GB/T 35273-2020)[12] consider medical and physiological data, biometric personal data as personal confidential information. Standards are crucial for bio-data security. With rapid progress of web technologies over the last few years and new issues emerging in related areas one by one, legislation, being subject to rigid procedures, is obviously a laggard. Therefore, standards are used in practice largely to settle and standardize specific issues. The Chinese Government and market players have also developed a number of standards on collecting and protecting personal biological data. Thus, the Telecommunication Terminal Industry Forum Association issued in 2020 a group standard "Specifications for minimum required evaluation of personal data to be collected and used by APP: data on persons"[13]. According to China's Standardization Law[14], a group standard is the one jointly developed by a civil society organization under the law to satisfy market demand and support technological innovation and coordination between the relevant market players as agreed between the organization's members or presented for voluntary acceptance under the organization's statute, and designed largely by actors with a certain degree of influence over the industries in question.

Because of the late emergence of personal data legislation in China, provisions for protection of individuals' biological data are still scattered across sectoral laws. Though the adoption of the Law on Personal Data Protection has filled some legal gaps in specific areas, its content is still dominated by broad provisions on personal data collection, usage and processing while multiple standards developed in response to practical needs, albeit more detailed, are not binding and systematic.

3.2. Existing legal gaps

Limited computing and storage capacities allow to upload and store large amounts of personal data on platforms while a majority of wearable devices

[12] Available at: http://nic.swu.edu.cn/__local/1/FE/8B/5DC92A975E617561B685BDDE3DA_B7B6D500_FE10A.pdf (accessed: 19.06.2024)

[13] Available at: https://www.ttbz.org.cn/Pdfs/Index/?ftype=st&pms=40991 (accessed: 19.06.2024)

[14] Available at: http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-11/04/content_2031446.htm (accessed: 20.06.2024)

do not enable user control for preventing personal risks in these processes such as timely request for, correction, deletion or withdrawal of consent. Where users' personal data are uploaded to a cloud, violations cannot be stopped by powering off or switching off the device since data circulating between several data controllers are aggregated in different directions at different levels under specific scenarios, sectoral needs and business models [Xu T., 2018: 169]. Health care services provided by wearable devices such as Apple HealthKit, Google Fit, Huawei Hi Health etc. rely on big data analysis to collect large amounts of personal data on users' health in real time, as well as to monitor, screen and prevent a wide range of health issues. However, few people believe they have a right to decide what personal information will be collected by wearable devices and how it will be used. Obviously, consent is at the core of personal data protection in wearable devices [Man H., Guo L., 2023: 121]. Firstly, such consent is a manifestation of the party's autonomous will. Smart wearable devices can perform medical operations for physical health monitoring or detection of potential health problems where there is medical agreement between the user and the data processor, with the latter required to seek prior consent since the user is autonomous. On the other hand, wearable devices collect large amounts of medical data from the human body in real time and by providing health care services to users become a tool for medical research. To guarantee the user's rights and interests as a subject and to seek consent, the theory should go back to considerations on the duties of health personnel during the Second World War — Permissible Medical Experiments of The Nuremberg Code (1947): "The voluntary consent of the human subject is absolutely essential. This means that the person involved should have legal capacity to give consent; should be so situated as to be able to exercise free power of choice, without the intervention of any element of force, fraud, deceit, duress, overreaching, or other ulterior form of constraint or coercion; and should have sufficient knowledge and comprehension of the elements of the subject matter involved as to enable him to make an understanding and enlightened decision"[15].

The meaning of the term "consent" still needs to be specified in the effective Chinese law. As applied to wearable devices, the user's consent primarily refers to private domain, with para 1, Article 13 of the Law on Personal Data Protection ruling that data processors may process personal data upon a person's consent while under para 4, Article 13, no user con-

[15] Available at: https://cirp.org/library/ethics/nuremberg/ (accessed: 20.06.2024)

sent is required in emergency situation where someone's life and health are at stake[16]. While not an issue in the traditional production sectors, it is a problem in the industry of wearable devices widely used in medicine and health care where the user has a discretion in respect of medical interventions and should be able to independently decide whether the interests of his health prevail over those of his personal data, since users are often as much fearful of disclosure or unauthorized use of data as of any disease. The terms applicable to mandatory data processing in emergency should be made more specific. As the personal data subject cannot control whether his medical data is sent while instantly generated data such as pulse, blood pressure, body temperature as well as ECGs, brain waves etc., are no longer filtered by the brain before being sent by the subject and instead are automatically collected by the device, the data collection "consent" envisaged by the effective law is not sufficient.

At the same time, Article 4 of the Law on Personal Data Protection explicitly excludes anonymized data from protected personal information with an intent to fully realize the value of personal data for economic and social development once such data is cleared of individuality through the use of this mechanism, and thus to strike a balance between the use and protection of personal data [Zhang X., 2018: 48]. However, in practical terms it is often hard to tell whether personal data have been sufficiently anonymized as technologies and data used for re-identification are ever evolving to defy any forecast [Esayas S. Y., 2015: 3]. Some studies have shown that it is practically impossible to fully remove the risk of re-identification of anonymized personal data [Qi Y., 2021: 52]. Pursuant to Article 73 of the Law on Personal Data Protection, anonymization is a process whereby personal data are processed in such a way that they no longer identify a natural person and cannot be recovered. However, the Law contains no clue as to the extent of technical processing required to achieve the standard of non-identifiability and non-recovery.

Data processors will currently use personal data for profit-making largely under three business models: macro-economic decision-making; marketing of a specific business; and click bait [Shen J., 2022: 93]. Meanwhile, data likely to be used for the said purposes are practically impossible to anonymize, especially in areas such as user profiles and personalized recommendations [Ding X., 2019: 82]. The more detailed and complete are

[16] Available at: https://xxzx.lfyjzjxy.com/uploads/editor/98/0f4bdfcab2389b06ae0d5b2fa99753.pdf (accessed: 20.06.2024)

personal details contained in data, the more accurate are the outcomes obtained through an algorithm and thus its contribution to the accuracy of marketing. Thus, from the data processor's perspective, personal data anonymization is paradoxical: if data is not anonymized, there is no way to disseminate and use personal information; meanwhile, anonymized data that could be disseminated and used have no value. A strife towards absolute data security is clearly not the only purpose of law: it is equally important to promote the use of information and data, and to support the digital economy. Ideally, there should be a balance between data security and conveniency of data usage.

4. Proposals to improve the law and address gaps

4.1. Specifying legal provisions for informed consent

Despite China's effective laws clearly establish the principle of informed consent, the detailed provisions on personal data collection by wearable devices are in a sense inadequate, only to complicate adaptation to new situations and risks in the context of ongoing progress of modern information technologies. With regard to specific rules to seek consent, it is proposed to: firstly, allow for users' right to consent in substance; for documents such as data privacy, downloading and exchange statements, provide for the regime of partial consent or full refusal instead of full consent, with users to choose either option depending on their needs or preferences while applications should not interfere with or limit the use of different health management services provided by wearable devices if the user has opted for partial consent or full refusal. Secondly, health data and other physiological information such as cardiac rate, blood oxygenation, blood pressure, body temperature, brain waves, ECG etc. collected by sensors and IOT units on wearable devices, once tracked and integrated, can easily disclose the user's past clinical record and particular states of health. Pursuant to para 2, Article 28 of the Law on Personal Data Protection, the following three conditions are to be met for processing sensitive personal data: specific purpose; reasonable necessity; rigorous protective measures. With regard to wearable devices, data processors are required to specify the type and amount of biometric data they collect and the underlying purpose. Since the Chinese law does not establish a list of specific purposes of biometric data collection, operators should explain the purpose of each biometric data unit to be collected in authorization requests in simple

language understandable to users. Thus, if the operator only indicates that "certain part of information will be used for gaming functionalities", the requirement of "specific purpose" will not be met; it should be stated instead that information will be used to support a certain functionality in the specific part of the game, with vibration, animation etc. used to clearly tell the user that full awareness is required before the "agree" button is pressed. It should be noted that at the data usage stage the data processor should process personal medical data to the minimum extent required to achieve a specific user-allowed purpose. Under Article 14 of the Law on Personal Data Protection and Article 38 of the Policy for Ethical Review of Bio-Medical Research Involving Human Subjects[17], a new written user consent should be sought where the specific purpose, method and type of data processing, as well as the program, amount and content of research have been changed. Individual users should also be aware of their rights and give attention to the specific terms of service, personal data collection/privacy protection agreement for VR applications, and report equivocal or unfounded terms to consumer associations and other bodies while the government should provide for convenient ways to lodge complaints.

4.2. Helping users to truly exercise the right to withdraw consent to personal data processing

While the Law on Personal Data Protection stipulates that consent to personal data processing may be withdrawn[18], this makes little practical effect. In this regard, application developers may be required to clearly specify the user's right to withdraw consent and the path to the relevant button for the user to decide whether to give or withdraw consent, and to ensure the ease of the button's use in absence of artificial obstacles (like heaping it up with settings). Firstly, where the data processor has been changed at the data usage stage as a result of liquidation following merger,

[17] Available at: https://www.gov.cn/zhengce/2016-10/12/content_5713806.htm (accessed: 23.06.2024)

[18] Article 15. Where personal data are processed upon a natural person's consent, such consent may be withdrawn. The personal data processor should arrange for a convenient way to withdraw consent. Withdrawal of consent shall not affect the validity of personal data processing operations consented by the natural person before such withdrawal. Article 16. The personal data processor should not deny the provision of goods or services on the basis that a natural person does not give or withdraws consent to personal data processing, except where personal data processing is required to provide goods or services.

division or bankruptcy, the name and contact details of the data recipient should be clearly communicated to the user with the help of animation or voice message within a prior reasonable period based on the principle of specific purpose and the user's reasonable trust in the data processor, with the user entitled to withdraw consent. Secondly, since users assume the main risk under the health management scenario, the user has a discretion to withdraw consent to physiological data processing and may exercise the right to remove unnecessary, irrelevant or obsolete physiological data processed and controlled by the data processor. Thirdly, users have the right to withdraw from medical research projects at any time while data processors should timely stop processing personal medical data following a withdrawal request and timely provide feedback to the data subject. Withdrawal of consent by the user does not affect the validity of prior operations to process personal health data consented by the user. Once the purpose of research has been reached, the data processor should step in to delete such data. Fourthly, it is proposed to implement arrangements for the "loss" of device, that is, where a wearable device has been lost, stolen, abandoned etc., convenient and fast channels will be provided to users to report the loss and lodge complaints, with the device to be automatically "blocked" and the stored personal data timely deleted in the background mode, once the event of loss has been conformed.

4.3. Improving legal provisions for emergency personal data processing

Constraints that make it impossible to obtain data processing consent in a situation of major risk to human life and health can do a considerable harm to users. There is only one legal basis to force wearable devices to process personal medical data, that is, para 4, Article 13 of the Law on Personal Data Protection: "Life and health of natural persons should be protected in emergency". Researchers believe that the Civil Code and the Law on Personal Data Protection reflect pluralistic rules of consent [Xiao X., 2022: 176]. However, the above law-protected interests and rights to protection of life and health, as well as the right to information belong to users who, given their compliance with social order, morals and public interests, have a discretion to decide on their affairs and even life, and thus cannot neglect their own will. In our view, paragraph 4, Article 13 of the Law on Personal Data Protection is close to *negotiorum gestio* (Article 979, Civil Code of China) whereas processing personal medical data to avoid

harm to the user's rights and interests is *negotiorum gestio* because of the need to protect the user's interests presumed to be the user's intent. To avoid unauthorized processing of data by smart wearable devices, the following conditions should be met: firstly, major risk: user's life and health should be at risk; secondly, data processing urgency; and, thirdly, data minimization principle. From the perspective of comparative law, GDPR clearly defines the principle of data minimization[19].

4.4. Dynamic anonymized data assessment

The consequences of de-identification are by no means static since they are rooted in continuous technological progress and massive buildup of data and information. The Article 29 Working Party (2014a) analyses the force and limits of anonymization techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them[20]. ICO call for views: Anonymization, pseudonymization and privacy enhancing technologies guidance chapter 4 (Accountability and governance): "Your governance procedures should address what you will do if you are concerned that the risk of re-identification has increased, e.g., due to technological developments or increased availability of additional information that when linked to the anonymized data may facilitate re-identification. You should consider introducing measures to mitigate these risks"[21].

Thus, the ranking of de-identified personal data should be dynamic, with data processors required to keep the de-identification effect under permanent control through a risk assessment mechanism implemented to specify the systemic processes, subjects of supervision and liability for regular assessment of risks regarding de-identified personal data [Xia Q., 2022: 102]. The risk of re-identification of de-identified personal data may vary depending on the evolution of information environment, data users, technological development levels and other pertinent factors. Thus, data processors should re-assess the re-identification risk on a permanent basis or following changes to the relevant factors, with de-identification to be performed again based on assessment results.

[19] Available at: https://gdpr-info.eu/art-5-gdpr/ (accessed: 25.06.2024)

[20] Available at: https://www.aepd.es/documento/88197.pdf (accessed: 25.06.2024)

[21] Available at: https://www.lexology.com/library/detail.aspx?g=f443dc16-49e8-49e6-b2be-cdd59c04e884 (accessed: 26.06.2024)

In addition, once explicit identifiers were processed with the help of technology, the data processor must store additional data separately and not disclose them together with core information. For example, where all full names in a large personal data block are replaced with a specific type of identifiers using pseudonymization, the data processor is required to store separately and withhold any additional data that allows to recover full names. Meanwhile, the data processor is required not to perform re-identification and, if personal data with removed explicit identifiers have been transferred, contractually prohibit re-identification to the recipient (Han X., 2018: 72). Should the recipient re-identify data in violation of the contract with the data processor, he will assume liability. Should the recipient re-identify personal data by removing explicit data identifiers or by processing for other than originally specified purpose to the detriment of the rights and interests of personal data subjects, he will be liable to such data subjects for damages and other tort obligations. Data subjects may require compensation of damages both from data recipient and data processor. Once compensation was paid, the data processor has the right to recover damages from the recipient. Under Article 1197 of the Civil Code of China, the data processor shall assume joint liability in the event of a failure to act where he was or should have been aware of the data recipient's illegal conduct.

4.5. Innovative technologies to prevent hacking attempts

In response to the risk of personal data leakage and hacking attempts, wearable device manufacturers should introduce innovative technologies and take appropriate action to assume social responsibility. Conventional electronic devices (computers, smartphones, watches etc.) come with data protection technologies such as private data encoding, secure application and developer audit tools, access control and authentication technologies designed to limit data collection etc. Data protection in smart wearable devices should be based on unique data properties such as safer file types and formats for multi-modal data profiles collected by wearable devices, proprietary data collection modules added to wearable device hardware to characterize engagements with users for numerous aspects of biological information, as well as using several data authentication methods such as biometry and virtual identifiers to mitigate the risk of intrusion and fraud for wearable devices.

Conclusion

While a combination of smart wearable devices and applications is likely to satisfy users in their strife for entertainment and health as well as better living standards, these gadgets will keep watch over users round the clock to collect data that can attract advertisers, research institutions and even hackers. Over the last few years, the problem of data privacy and security has come under increasing scrutiny and, as individuals are becoming aware of the need for privacy and security, there is a need in tougher regulation of smart wearable devices from this perspective. Now that the technology of wearable devices is rapidly progressing, there is no assurance that it will expand across all spheres of life and work unless we guarantee that data collection does not undermine privacy and security. Market players should also join forces to ensure compliance of wearable devices with biometric data collection and processing requirements.

References

1. Ding X. (2019) User Profiles, Personalized Recommendations and Personal Information Protection. *Huan qiu fa lv ping lun* = Global Law Review, no. 5, pp. 82–96 (in Chinese).

2. Esayas S.Y. (2015) The role of anonymization and pseudonymization under the EU data privacy rules: beyond the "all or nothing" approach. *European Journal of Law and Technology,* no. 2, pp. 1–20.

3. Han X. (2018) Legal Regulation of Anonymous Information in the Era of Big Data. *Da lian li gong da xue xue bao (She hui ke xue ban)* = Journal of Dalian University of Technology (Social Science Edition), no. 4, pp. 64–75 (in Chinese)

4. Hu L. (2018) On the Architecture of Cyberspace and Its Legal Implications. *Dong fang fa xue*=Oriental Law, no. 3, pp. 87–99 (in Chinese)

5. Liu X. (2020) Patent Analysis of Global Wearable Medical Intelligent Devices Based on "Wisdom Buds". *Zhong hua yi xue tu shu qing bao za zhi*=Chinese Journal of Medical Library and Intelligence, no. 8, pp. 37–42 (in Chinese)

6. Man H., Guo L. (2023) Personal health information protection in wearable devices — a consent-centered study. *Fa xue lun tan*=Law Forum, no. 2, pp. 121–131 (in Chinese)

7. Qi Y. (2021) A Review of China's Personal Information Anonymisation Rules and Alternative Choices. *Huan qiu fa lv ping lun*=Global Law Review, no. 2, pp. 52–66 (in Chinese)

8. Song M., Xu S. (2020) Wearables as media: dataization and regulation of the body. *Xian dai chuan bo*=Modern Communication, no. 4, pp. 46–50 (in Chinese)

9. Shen J. (2022) The Rights Architecture and the Unfolding of the Rules of Data Property. *Zhong guo fa xue*=China Law Journal, no. 4, pp. 92–113 (in Chinese)

10. Tian Y., Zhang Y. (2021) The Protection of Personal Health Information in the Era of the Civil Code. *Bei jing hang kong hang tian da xue xue bao (She hui ke xue ban)*=Journal of Beijing University of Aeronautics and Astronautics (Social Science Edition), no. 6, pp. 47–58 (in Chinese)

11. Wei Z., Shi H., Cao T. (2020) Research progress of intelligent wearable devices at home and abroad. *Zhong guo yi xue zhuang bei* = China Medical Equipment, no. 10, pp. 18–21 (in Chinese)

12. Xu T. (2018) Privacy Dilemma and Remedy Path in the Age of Artificial Intelligence. *Xi nan min zu da xue xue bao (Ren wen she hui ke xue ban)*=Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition), no. 6, pp.166–170 (in Chinese)

13. Xu T. (2022) Data Intelligence Regulation: Privacy Risks and Protection of Wearable Devices. *Jiang xi she hui ke xue* = Jiangxi Social Science, no. 12, pp. 162–170 (in Chinese)

14. Xiao X. (2022) Pluralistic Consent Rules for Personal Information Processing — Understanding and Interpretation Based on the Consent Hierarchy System. *Zheng zhi yu fa lv*=Politics and Law, no. 4, pp. 158–176 (in Chinese)

15. Xia Q. (2022) Improvement of Notification Obligations and Dynamic Anonymization of Personal Information Protection in Cyberspace. *Jiang han lun tan*=Jianghan Forum, no. 3. pp. 95–103 (in Chinese)

16. Zhang X. (2018) Discussion on the Main Contradictions of China's Personal Information Protection Law Legislation. *Ji lin da xue she hui ke xue xue bao*=Journal of Social Sciences of Jilin University, no. 5, pp. 45–56 (in Chinese)

Information about the author

Li Yao — Doctor of Sciences.

The article was submitted to editorial office 05.07.2024; approved after reviewing 15.08.2024; accepted for publication 05.09.2024.