pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

Legal science field: Theory and history of state and law. History of legal doctrines

UDC: 342.7:342.738:004:614.2

PERSONAL DATA CONCERNING THE HUMAN BODY AS AN OBJECT OF SOMATIC RIGHTS

Istamova-Fayzullaeva Dilafruz Oybek kizi
PhD researcher, Department of Theory of State and Law, Tashkent State University of Law
E-mail: dilafruzkhon99@gmail.com
https://doi.org/10.5281/zenodo.20355284

Abstract.

This article examines personal data concerning the human body as an independent object of somatic rights within the theory of state and law. It argues that the legal protection of the body is no longer limited to direct physical interference, because contemporary digital systems increasingly translate bodily existence into health data, biometric identifiers, genetic information, physiological indicators and algorithmic body profiles. The study uses normative, comparative legal and systemic methods to clarify the relationship between bodily autonomy, human dignity, medical confidentiality, personal data protection and the emerging doctrine of somatic rights. The article demonstrates that body-related personal data has a dual legal nature: it is simultaneously information about a person and a digital representation of the person's physical integrity. On this basis, the article proposes safeguards such as purpose limitation, data minimization, necessity and proportionality of biometric processing, access and correction rights, traceability of access to medical records, and stricter limits on secondary use by employers, insurers and other third parties.

Keywords: somatic rights, bodily autonomy, personal data, health data, biometric data, genetic data, informational self-determination, medical confidentiality, human dignity, data protection

In contemporary legal systems the human body is increasingly mediated by data. A medical record, a biometric template, a genetic sequence, a wearable sensor reading or an algorithmic assessment of physical fitness is not a neutral technical trace. It is information derived from the person's body and capable of affecting the person's legal status, social opportunities, access to work, insurance, health care and even freedom from discrimination. Therefore, the question of personal data concerning the human body must be considered not only within the narrow framework of privacy or information law, but also within the broader category of somatic rights.

The relevance of this topic is determined by the transformation of bodily integrity in the digital era. Classical constitutional and civil-law doctrine usually associated bodily integrity with protection against physical violence, unlawful medical intervention or coercive treatment. However, the body can now be affected without being physically touched. When a person's health status is disclosed, a biometric identifier is stored without sufficient necessity, or genetic information is used for risk classification, the person's bodily autonomy is indirectly but substantially affected. In this sense, data about the body becomes a new legal frontier of somatic rights.

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

The aim of this article is to substantiate the category of personal data concerning the human body as an object of somatic rights and to determine the legal safeguards required for its protection. The research applies normative analysis, comparative legal analysis, systemic interpretation and legal construction. The normative method is used to examine constitutional, bioethical and data protection standards. Comparative analysis helps to identify common principles in European and Uzbek legal approaches. The systemic method reveals the interconnection between bodily autonomy, dignity, privacy and informational self-determination.

The literature on bioethics and human rights shows that human dignity, bodily autonomy and informed consent are central values in the legal regulation of the body. Beauchamp and Childress treat autonomy, non-maleficence, beneficence and justice as fundamental principles of biomedical ethics (Beauchamp & Childress, 2019). Andorno argues that human dignity can function as a common normative ground for global bioethics, especially where scientific or technological development creates risks for the person (Andorno, 2009). Brownsword emphasizes that technological governance should not displace human agency, because law loses its protective function when persons are reduced to objects of technical administration (Brownsword, 2008).

At the same time, privacy scholarship demonstrates that privacy is not merely secrecy. Solove explains privacy as a complex structure of protections against excessive collection, processing, dissemination and use of personal information (Solove, 2008). In the digital environment, the problem is not only that information may become public, but also that it may be aggregated, interpreted and used in ways that the person cannot reasonably control. This idea is particularly important for body-related data, because such data is often intimate, permanent and predictive. A biometric template or a genetic marker may reveal more than the individual expected and may continue to create legal consequences long after the original collection.

The concept of somatic rights is useful because it allows legal theory to connect physical and informational dimensions of the body. Somatic rights should not be understood only as rights concerning organ transplantation, reproductive technologies, sex reassignment or end-of-life decisions. These issues are important, but they do not exhaust the category. From the standpoint of the theory of state and law, somatic rights include the individual's power to preserve bodily integrity, make autonomous decisions about bodily interventions, control the social and legal use of bodily characteristics, and protect data generated from or about the body.

Personal data concerning the human body may be defined as any information relating to an identified or identifiable person that directly or indirectly describes, measures, identifies, predicts or evaluates the person's physical, physiological, genetic, biometric, reproductive or health-related characteristics. This definition is wider than ordinary medical data. It includes formal medical diagnoses, laboratory results and hospital records, but also facial images used for identification, fingerprints, voice patterns, DNA profiles, menstrual or reproductive data, data from fitness trackers, sleep indicators, heart-rate patterns and algorithmic inferences about health or bodily capacity.

This category has a dual legal nature. First, it is personal data, because it relates to an identifiable person. Secondly, it is a digital representation of the body, because its source, meaning and consequences are connected with the person's physical existence. The same information may therefore be protected simultaneously by personal data law, health law, medical secrecy, constitutional privacy and somatic rights. The somatic-rights approach does not replace data protection law; rather, it adds a bodily autonomy dimension to it. It asks not only whether data was processed lawfully, but also whether the processing respects the person as the holder of a body, dignity and agency.

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

International legal standards support this broader interpretation. The General Data Protection Regulation defines personal data broadly as information relating to an identified or identifiable natural person and specifically refers to factors of physical, physiological, genetic, mental, economic, cultural or social identity (European Union, 2016). The GDPR also defines genetic data, biometric data and data concerning health as separate categories and includes them among special categories of personal data whose processing is generally prohibited unless strict legal grounds and safeguards exist (European Union, 2016). This structure confirms that body-related data is not ordinary information; it belongs to a more sensitive legal layer.

The Oviedo Convention also connects private life and health information. Article 10 recognizes the right to respect for private life in relation to health information and the right to know any information collected about one's health (Council of Europe, 1997). The UNESCO Universal Declaration on Bioethics and Human Rights similarly emphasizes autonomy, consent, privacy and confidentiality in the application of medicine, life sciences and associated technologies (UNESCO, 2005). These instruments show that the body-data relationship is not purely technical. It is a matter of dignity and self-determination.

The case law of the European Court of Human Rights confirms that retention and disclosure of body-related information may interfere with private life. In S. and Marper v. the United Kingdom, the Court considered the retention of fingerprints, cellular samples and DNA profiles as an interference with the right to respect for private life (European Court of Human Rights, 2008). In Z v. Finland and I v. Finland, the Court stressed the fundamental importance of protecting medical data and the need for effective safeguards against unauthorized access and disclosure (European Court of Human Rights, 1997; European Court of Human Rights, 2008). These judgments are important for somatic rights because they show that the legal injury may arise from the informational use of bodily traces, not only from physical intervention.

Uzbekistan's constitutional framework also provides grounds for this approach. The Constitution of the Republic of Uzbekistan guarantees the inviolability of private life, personal and family secrets, protection of honor and dignity, and expressly recognizes the right to protection of personal data, including correction of inaccurate data and destruction of unlawfully collected data (O'zbekiston Respublikasi Konstitutsiyasi, 2023). The same Constitution recognizes the right to health and qualified medical care (O'zbekiston Respublikasi Konstitutsiyasi, 2023). These norms create a constitutional bridge between health, dignity, privacy and personal data protection.

The Law of the Republic of Uzbekistan "On Personal Data" applies to relations arising from the processing and protection of personal data regardless of the means of processing, including information technologies (O'zbekiston Respublikasi, 2019/2026). It establishes principles and conditions of processing, duties of the owner and operator, confidentiality requirements, and special rules for biometric and genetic data. This is particularly relevant because biometric and genetic data are directly connected with the human body and are difficult, and sometimes impossible, to replace if compromised.

The Law "On Protecting the Health of Citizens" also supports the somatic-rights dimension of body-related data. It recognizes the citizen's right to receive necessary information about his or her health, including examination results, diagnosis, prognosis, treatment methods, risks, types of medical intervention and consequences (O'zbekiston Respublikasi, 1996/2026). This means that body-related data protection must not be reduced only to confidentiality. It must include the subject's access to his or her own body-related information and the ability to understand the legal and medical consequences of such information.

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

The legal importance of body-related data can be illustrated through several groups. Health data describes the person's physical or mental condition. Genetic data contains inherited or acquired characteristics and may reveal information not only about the individual but also about biological relatives. Biometric data is used to identify the person through bodily features and is especially risky because the person cannot change fingerprints or facial geometry in the same way as a password. Reproductive and sexual-health data relates to deeply intimate aspects of bodily autonomy. Wearable and sensor data may look harmless, but it can reveal sleep, stress, pregnancy, disability, movement, heart rhythm and other bodily conditions. Finally, algorithmic inferences may create profiles about a person's health risks or physical capacity even when the original data was not collected as medical data.

The following table summarizes the main categories of personal data concerning the human body and the safeguards required from the standpoint of somatic rights.

Table

Personal data concerning the human body and somatic-rights safeguards

Type of data	**Connection with the human body**	**Somatic-rights risk**	**Necessary legal safeguard**
Health data	Diagnosis, examination results, treatment history and prognosis	Disclosure may affect dignity, work, insurance, family life and social status	Medical confidentiality, access right, purpose limitation, secure storage
Biometric data	Fingerprint, facial image, voice, iris, dactyloscopic data or other identifiers	Irreplaceable bodily identifiers may enable continuous surveillance	Necessity, proportionality, alternatives, strict retention limits
Genetic data	Inherited or acquired genetic characteristics obtained from biological material	Predictive information may affect the person and biological relatives	Special legal basis, genetic counselling, anti-discrimination guarantees
Reproductive and sexual-health data	Pregnancy, fertility, reproductive technology, sexual health and related treatment data	High risk of stigma, discrimination and violation of intimate autonomy	Enhanced confidentiality, limited access, informed consent and remedy mechanisms
Wearable and physiological data	Heart rate, sleep, stress, movement, body temperature and other sensor readings	Commercial or employment use may create hidden health profiles	Transparency, data minimization, prohibition of incompatible secondary use
Inferred body profiles	Algorithmic predictions about health risks, capacity, disability or behaviour	Automated decisions may restrict opportunities without medical verification	Explainability, human review, contestation right, impact assessment

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

Source: author's development.

The table shows that the same body-related data may perform a useful function and at the same time create a serious rights risk. For example, biometric identification may prevent fraud, but if it becomes a universal administrative requirement, it may normalize the collection of irreplaceable bodily identifiers. Wearable data may help a person manage health, but when transmitted to employers or insurers it may become a tool for classifying bodies according to productivity, risk or cost. Therefore, the decisive question is not whether body-related data may be processed at all. The decisive question is whether the processing is legally necessary, proportionate, transparent and oriented toward the rights of the data subject.

The somatic-rights approach also changes the meaning of consent. Consent remains important, but it cannot be treated as a universal justification for every processing operation. In health care, employment, insurance or state services, the person may not always be in an equal position. The formal signature of consent may hide factual dependence. For this reason, consent to body-related data processing must be specific, informed, revocable and accompanied by real alternatives where possible. Where the processing is mandatory by law, the absence of consent must be compensated by strong legal safeguards, independent oversight and effective remedies.

Another important issue is secondary use. Body-related data is often collected for one legitimate purpose, such as diagnosis, treatment, public health, identity verification or scientific research. However, the same data may later become attractive for other purposes: employment screening, insurance pricing, migration control, targeted advertising, profiling or commercial analytics. Such purpose drift is especially dangerous for somatic rights because the individual may lose control over the social meaning of his or her body. The principle of purpose limitation must therefore be interpreted strictly in relation to body-related data.

Data minimization is equally essential. A public or private institution should not collect the maximum amount of bodily data merely because technology makes it possible. The legal question must be formulated differently: what minimum information is necessary to achieve the specific legitimate aim? If identity can be confirmed by a less intrusive method, compulsory biometric processing is not justified. If a workplace only needs confirmation that a person is fit for a particular task, the employer should not receive the full diagnosis or detailed medical history. Such separation between necessary functional information and detailed medical information is a key safeguard of somatic rights.

Traceability of access is another procedural guarantee. In paper-based systems, unauthorized access to medical information may be difficult to detect. In digital systems, however, every access can and should be logged. A person should be able to know which institution, official or medical worker accessed body-related data, when, and for what purpose, unless a narrowly defined legal exception applies. This requirement transforms confidentiality from an abstract principle into an enforceable mechanism. It also supports accountability of data controllers and operators.

The protection of body-related data must also include the right of access, correction and deletion where the legal grounds for storage no longer exist. The subject should not remain a passive object of databases. Where data about the body is inaccurate, outdated or collected without legal basis, it may cause direct harm: an incorrect diagnosis may affect treatment; an inaccurate biometric record may cause identification problems; an erroneous algorithmic health profile may restrict employment or services. The subject's procedural rights are therefore part of the substance of somatic rights.

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

A separate challenge arises from algorithmic inferences. Modern systems may infer pregnancy, disability, stress level, disease risk or physical performance from indirect data. Such inferences may be produced without a medical examination and without the person's awareness. From the standpoint of somatic rights, inferred body profiles should not be treated as less important simply because they are probabilistic. If they are used to make decisions affecting the person, they must be subject to transparency, human review and contestation. The right to challenge an algorithmic body profile should be recognized as a procedural component of bodily autonomy.

Theoretical analysis allows us to formulate several legal features of personal data concerning the human body. First, it has an intimate character because it is linked with the person's physical and psychological existence. Secondly, it has a persistent character because some identifiers, especially genetic and biometric data, cannot be changed. Thirdly, it has a predictive character because it may reveal future health risks or bodily capacities. Fourthly, it has a relational character because genetic and family health data may concern other persons as well. Fifthly, it has a status-forming character because it may influence employment, social protection, insurance, medical treatment and access to services.

These features justify a stricter legal regime. Ordinary personal data protection rules are necessary but not always sufficient. Body-related data requires an additional somatic-rights test. Such a test may include five questions: whether the processing is connected with a legitimate and clearly defined aim; whether less intrusive means are available; whether the person has access to and control over the data; whether the processing may lead to discrimination or bodily stigmatization; and whether there are effective remedies for unlawful processing or disclosure. If the answer to these questions is negative, the processing should not be considered compatible with somatic rights.

For Uzbekistan, this approach may be used in legislative and administrative reforms concerning digital health, biometric identification, electronic medical records, reproductive health services and public databases. The Law "On Personal Data" already contains important provisions on special, biometric and genetic data, confidentiality and the rights of the data subject. However, the rapid development of digital services requires further concretization. It would be useful to introduce a doctrinal and regulatory category of "personal data concerning the human body" or at least to elaborate sector-specific rules that combine data protection, medical secrecy and bodily autonomy.

The first normative proposal is to clarify the status of body-related data in legislation and subordinate regulations. Such clarification should include health data, genetic data, biometric data, reproductive and sexual-health data, wearable physiological data and algorithmic inferences concerning bodily status. This does not mean that every category must have identical rules. Rather, each category should be assessed according to its sensitivity, permanence, predictive power and potential consequences for the person.

The second proposal is to strengthen the necessity and proportionality requirement for biometric and genetic processing. Biometric collection should not become a default administrative convenience. It should be allowed only where the legal aim cannot be achieved by a less intrusive method, where retention periods are limited, where storage is secure, and where non-biometric alternatives remain available whenever possible. Genetic data should be processed under even stricter conditions because it may reveal information about relatives and future health risks.

The third proposal concerns access and explanation. Individuals should have a clear right to receive information about what body-related data is processed, for what purpose, by whom,

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

for how long, and with what legal consequences. In the field of health, this right should include examination results, conclusions, diagnoses, risk assessments and the possibility to receive copies in electronic or paper form. Where algorithmic tools are used, the person should be informed about the logic and significance of the assessment in understandable language.

The fourth proposal is to limit secondary use by employers, insurers and commercial actors. The fact that a person's bodily data exists in a database should not make it available for purposes unrelated to the original legitimate aim. In particular, employers should receive only the minimum conclusion necessary for occupational safety or legal compliance, not detailed medical records. Insurers and commercial platforms should not use body-related data in ways that create unfair exclusion, hidden discrimination or economic pressure on vulnerable persons.

The fifth proposal is to create effective remedies. Protection of somatic rights requires not only prohibitions but also practical mechanisms: internal complaint procedures, independent supervision, administrative liability, compensation for harm, correction and deletion mechanisms, and judicial review. The person must be able to contest unlawful collection, excessive retention, unauthorized disclosure, inaccurate body-related records and automated decisions based on bodily profiles.

The originality of the present approach lies in treating body-related personal data as a bridge between two legal fields that are often discussed separately: somatic rights and personal data protection. Data protection law provides the technical and procedural language of processing, controllers, consent, access, correction and security. Somatic rights provide the substantive human-rights meaning of the body, dignity, autonomy and physical integrity. Their combination creates a more complete legal model for the digital age.

In conclusion, personal data concerning the human body should be recognized as an object of somatic rights because it represents the body in legal and digital space. Protection of the body today requires protection not only against direct physical interference, but also against uncontrolled collection, storage, analysis, disclosure and secondary use of bodily information. Health data, biometric identifiers, genetic information, reproductive data, wearable indicators and algorithmic body profiles can affect dignity, autonomy, equality and access to social goods.

The analysis leads to three main conclusions. First, body-related personal data has a dual nature: it is information about the person and at the same time an informational extension of bodily integrity. Secondly, the legitimacy of processing such data depends on legality, necessity, proportionality, confidentiality, transparency, access and effective remedies. Thirdly, the theory of somatic rights should be developed beyond traditional bioethical issues and should include the informational dimension of the body. Only such an approach can ensure that digitalization of health care, identification and public administration serves the human being rather than reducing the human body to a resource for databases and algorithms.

References:

1. Andorno, R. (2009). Human dignity and human rights as a common ground for a global bioethics. Journal of Medicine and Philosophy, 34(3), 223-240. https://doi.org/10.1093/jmp/jhp023
2. Beauchamp, T. L., & Childress, J. F. (2019). Principles of biomedical ethics (8th ed.). Oxford University Press.
3. Brownsword, R. (2008). Rights, regulation, and the technological revolution. Oxford University Press.

pISSN:2349-5707 Volume:13,Issue 5, May -2026 eISSN:2349-5715

4. Council of Europe. (1997, April 4). Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. https://rm.coe.int/168007cf98
5. Council of Europe. (2018). Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+). https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
6. European Court of Human Rights. (1997). Z v. Finland, Application No. 22009/93. https://hudoc.echr.coe.int/eng?i=001-58033
7. European Court of Human Rights. (2008). I v. Finland, Application No. 20511/03. https://hudoc.echr.coe.int/eng?i=001-87510
8. European Court of Human Rights. (2008). S. and Marper v. the United Kingdom, Applications Nos. 30562/04 and 30566/04. https://hudoc.echr.coe.int/eng?i=001-90051
9. European Union. (2016). 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. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
10. Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A, 374(2083), 20160360. https://doi.org/10.1098/rsta.2016.0360
11. Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (Eds.). (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.
12. O‘zbekiston Respublikasi. (1996/2026). On protecting the health of citizens, Law No. 265-I, 29.08.1996 (current edition). https://lex.uz/en/docs/6813966
13. O‘zbekiston Respublikasi. (2019/2026). On personal data, Law No. O‘RQ-547, 02.07.2019 (current edition). https://lex.uz/docs/4831939
14. O‘zbekiston Respublikasi Konstitutsiyasi. (2023). The Constitution of the Republic of Uzbekistan. https://lex.uz/en/docs/6451070
15. Solove, D. J. (2008). Understanding privacy. Harvard University Press.
16. UNESCO. (2005). Universal Declaration on Bioethics and Human Rights. https://unesdoc.unesco.org/ark:/48223/pf0000146180
17. Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 2019(2), 494-620. https://doi.org/10.7916/cblr.v2019i2.3424