

Data Protection Under Review of Constitutional Court: Administrative Databases Directly Accessible to Public Authorities

Aleksandrs Potaičuks

Riga Graduate School of Law
Strelnieku iela 4A
Riga LV-1010, Latvia
aleksandrs.potaicuks@rgsl.edu.lv

Abstract: The development and use of administrative databases accelerate administrative and sometimes even criminal proceedings within public authorities. However, the increased data storage and free circulation of data pose a challenge to the protection of personal data and, thus, to the privacy of individuals. The focus of this article is the constitutional control of legislation that mandates the storage and processing of personal data—the review of legislative acts themselves, not their application. This article first presents two leading cases of the Constitutional Court of Latvia; second, it analyses the scope of the review and the constitutional articles protecting personal data in state-held databases; and third, the article analyses the legal problems that led to the annulment of the relevant national provisions. Finally, the author generalises on the lessons of the two judgments and similar judgments of the Court of Justice of the European Union and the European Court of Human Rights for future administrative databases directly accessible to public authorities and discusses the particular considerations that any legislator must take into account when mandating the storage of certain types of personal data in administrative databases.

Keywords: *constitutional law, databases, data protection, privacy, proportionality of state measures, ReNEUAL model rules*

1. Introduction

The digital age has opened doors to an ever-increasing flow of information (Sarat, Douglas & Umphrey, 2012, p. 8), much of which is, by its nature, personal data. However, the increased data storage and processing of personal data pose a challenge to the protection of personal data protection and, consequently, to the privacy of individuals.

One example is public databases accessible to public authorities. Governments are now creating new databases and registers to improve government processes: to adopt administrative decisions, such as granting pensions, driving licenses, or construction permits; or to supervise private individuals, such as tax-paying discipline or compliance with restrictions imposed on individuals by national laws or authorities. In some cases, such databases are even used to shame or deter individuals from certain behaviours, for example, by publishing information about athletes who have breached anti-doping rules. The most recent example of this is disputed in the European Court of Justice in the case of *NADA and Others* where the Court was asked to assess whether the General Data Protection Regulation precludes a national provision providing for the disclosure of the names of individuals who have breached anti-doping rules (*SO v. Nationale Anti-Doping Agentur Austria GmbH (NADA) and Others* [2023]).

Usually, the inclusion of personal data in state-held databases is provided for by laws adopted by national parliaments, which define the type of personal data and how the data should be stored in state administrative databases. The inclusion of such personal data in state-held databases has been challenged in two landmark decisions of the Constitutional Court of Latvia. One case relates to the storage of personal data of an acquitted person in the archives of the Punishment Register for their entire lifetime (Constitutional Court, 2022-09-01), and the second case concerns the public accessibility of information on fines imposed on a person for road traffic offenses that have not been paid within the period specified by law (personal data available in the State Register of Vehicles and Drivers Thereof) (Constitutional Court, 2018-18-01).

From a methodological point of view, this article aims to focus on case-law, providing considerations that any European legislator should take into account during the legislative process in order to avoid jeopardising fundamental rights. However, this article has its research limitations: it

is not intended to address the practical or technical aspects of database development, people's behaviour in this regard, or state liability. Rather, the article deals with the method of developing laws related to the digitalisation of society and privacy and provides further discussion on the ReNEUAL model rules on EU administrative procedure for administrative databases directly accessible to public authorities (Hofmann, Schneider & Ziller, 2014).

2. Competence of the Constitutional Court

The Constitutional Court in Latvia is a judicial body with the authority to review the conformity of legislation with higher legal norms, in particular with the Constitution. Its rulings have generally binding force (*erga omnes*) (Pleps, Pastars & Plakane, 2022, p. 515), and the Constitutional Court thus functions as a “court of laws.” Such courts in Europe typically have the power to review both whether the content of the legislation in question violates the established right and whether special legislative procedures (due legislative process) were followed in adopting the law (Bar-Siman-Tov, 2012, p. 271).

Regarding the content (personal data) published in administrative databases, it should be emphasised that, in Latvia, national legislation provides that information systems, their operational procedure as well as the information included in the information systems shall be established on the basis of external regulatory enactments (laws) (Law on State Information Systems, Art. 5). Similar requirements are derived from the jurisprudence of the European Court of Human Rights, since operations with personal data amount to an interference with private life and such interference must be “in accordance with the law” (*Shimovolos v. Russia* [2011]). Thus, constitutional courts play an important role in overseeing administrative databases from the perspective of the constitutionality of laws.

3. Clashes between two competing interests: Public administration and protection of privacy

3.1 Case no. 2018-18-01: Demerit points

The first case concerned a demerit point system that collects information on road traffic offences such as speeding, failure to wear a seat belt, failure to stop at a traffic light, drink-driving, etc. A national administrative database obliged the State Register of Vehicles and Drivers to collect negative points for road traffic offences and made this information available to the public in order to deter drivers from committing repeat offences.

The applicant applied to the Constitutional Court, and in his application explained that he had eight penalty points for traffic offences registered in the state database. This information was made available to several merchants for the re-use of public sector information and, consequently, anyone could access it for a fee. Under the contested norm and in practice, this information had the status of “generally accessible information” and was, therefore, widely available to the public. However, this information should have been protected under the General Data Protection Regulation and the applicant argued that the contested provision violated his right to the inviolability of private life, as enshrined in Article 96 of the Constitution (Constitutional Court, 2018-18-01, pt. 2).

The contested norm, Section 141, paragraph 2 of the Law on Road Traffic, stated:

Information on a vehicle owned by a legal person, except for the information specified in Paragraph one of this Section, on the rights of a person to drive vehicles, on the fines imposed on a person for offences in road traffic which have not paid within the time period specified in the law, and also any other information contained in the State Register of Vehicles and Drivers Thereof and the State Information System of Tractor-type Machinery and Drivers Thereof shall be treated as generally accessible information. (Law on Road Traffic, Sec. 141(2))

The idea behind this regulation, as explained by the parliament, was twofold. On the one hand, it enabled to provide transport and taxi companies with information on drivers so that they could select trustworthy employees. On the other hand, the contested norm had a preventive function: it aimed to deter people from committing road traffic offences. In general, therefore, the norm promoted road safety. (Constitutional Court, 2018-18-01, pt. 3)

3.2 Case No 2022-09-01: Personal data of an acquitted person

The second case concerned information in the Punishment Register, which accumulated information on initiated criminal proceedings; persons who had committed a criminal offence; the progress and results of pre-trial investigations and criminal proceedings, etc. (including information that a person had been acquitted in criminal proceedings). In other words, if a person was acquitted in criminal proceedings, this information about the person was recorded in the Punishment Register.

The constitutional review was initiated at the request of the Administrative District Court. The administrative case, however, was initiated by a person acquitted in a criminal case who asked the Administrative District Court to recognise the actual action of the Information Centre of the Ministry of the Interior, that is, the storage of information on this person in the Punishment Register, as unlawful and to compensate the person for non-pecuniary damage. In its application to the Constitutional Court, the Administrative District Court stated that, according to the contested norm, information on an acquitted person must be kept in the criminal record for the entire life of that person. It is alleged that such a legal regulation disproportionately restricts a person's right to inviolability of private life, enshrined in Article 96 of the Constitution, as it is incompatible with the aims for which the Punishment Register was established and with the principles governing the processing a natural person's data in the field of criminal law. (Constitutional Court, 2022-09-01, pt. 2)

The contested norm, Section 23, paragraph 1 of Punishment Register Law, stated:

Information regarding a person whose criminal record has been set aside or extinguished, against whom the initiated criminal proceedings have been terminated, regarding an acquitted person, regarding a person on whom the imposed compulsory measure of correctional nature has been executed, a person on whom the imposed compulsory measure of medical nature has been revoked—for one year after information has been received from the Register of Natural Persons regarding the death of the person, however, not longer than 100 years after birth of the person, is stored in the archives database of the Punishment Register. (Punishment Register Law, Sec. 23(1))

The Parliament, as the adopter of the contested provision, explained that the storage of this information was intended for archival purposes. Firstly, it allows the authorities to confirm that the person has been acquitted in a criminal case. Secondly, the register allows the individual to obtain an official and reliable certificate to prove to others that he or she has been acquitted in a criminal case. The Parliament also explained that an acquittal does not mean that the situation can never change: the criminal case may, under certain circumstances, be reopened. (Constitutional Court, 2022-09-01, pt. 3)

Both cases concerning administrative databases thus underline the twofold objective of public law: firstly, to ensure that the measures in question promote the effective performance of public duties and, secondly, to ensure that the fundamental rights of private individuals are respected (Hofmann, Schneider & Ziller, 2014, p. 4). In the review procedure of the Constitutional Court, these two can be seen as competing interests that have taken the form of the existing legislation. It is therefore up to the Constitutional Court to resolve this conflict of interests in accordance with fundamental rights.

4. The scope of the right to private life covers entries in state administrative databases

Methodologically, in its jurisprudence, the Constitutional Court first examines whether the measure (legislative act) is covered by the relevant fundamental right, namely the right to private life under Article 96 of the Constitution. Only then does the Constitutional Court assess whether this right has actually been restricted. This approach is similar to that used by the European Court of Human Rights in cases concerning the right to private life (see, e.g., *Gaughran v. The United Kingdom* [2020]).

The norm of higher legal force (fundamental right): Article 96 of the Constitution:

Everyone has the right to inviolability of his or her private life, home and correspondence.

In cases involving state-held databases, the Constitutional Court (2015-14-0103, pt. 15) has held that Article 96 (the right to private life) also protects the processing of personal data.

In this context, the Court underlined that the protection of personal data must be ensured in any processing of personal data, including the collection and storage of personal data relating to physical and social identity (Constitutional Court, 2015-14-0103, pt. 15). This includes the collection and storage of personal data in the course of criminal proceedings and even after the criminal proceedings have been concluded or terminated (Constitutional Court, 2022-09-01, pt. 10). The inclusion of such personal data in the criminal record database, as well as the disclosure of such data, amounts to the processing of personal data (Constitutional Court, 2022-09-01, pt. 11). In this case, the length of time for which personal data is kept in the public database must be taken into account, as it leads to a restriction of the right to private life (Constitutional Court, 2022-09-01, pt. 18).

The legislator is responsible for creating such a legal framework that ensures that legal measures for the processing of personal data are appropriate for their intended purpose (Constitutional Court, 2018-18-01, pt. 15.1). Similarly, the legal framework for the public disclosure of personal data (including the establishment of a special status for the information, such as “generally available” information in the state-held database) relates to a person’s private life, so that such disclosure falls within the scope of the right to inviolability of private life (Constitutional Court, 2018-18-01, pts. 15.1 & 15.2.2).

In doing so, the Constitutional Court emphasised that the information defined in the contested norms, whether concerning the disclosure of a person’s demerit points or the storage of acquittal decisions in criminal cases, is related to the person’s private life, and the processing of such information therefore constitutes an interference with a person’s private life under the Constitution (Constitutional Court, 2018-18-01, pt. 15.3; cf. joined cases in *WM and Sovim SA v. Luxembourg Business Registers* [2022]). Thus, in general, it can be concluded that any legal norm that orders the storage of personal data in state databases is covered by the right to private life (Article 96 of the Constitution of Latvia or Article 8 of the European Convention on Human Rights). Given the context, it is possible to extend this jurisprudence to any situation where the legislator obliges to store personal data in state administrative databases, for example, personal data in commercial registers, land registers, family registers, tax registers, registers of declarations of financial interests, public health registers, etc.

In addition, it is worth mentioning that, in a similar way, state administrative databases and registers are being scrutinised by the Court of Justice of

the European Union (CJEU). In particular, the Court has examined cases concerning the publication of declarations of private interests by natural persons working in the public service;¹ registries of beneficial ownership;² Passenger Name Record data of air passengers;³ listing persons considered by the Finance Directorate to be “front-men” (fight against tax fraud);⁴ personal data in companies register;⁵ establishment and use of databases containing biometric data;⁶ transferring personal tax data from the national database;⁷ publication of information on beneficiaries of agricultural aid;⁸ public access to personal data relating to penalty points imposed for road traffic offences;⁹ publication of table concerning breaches of anti-doping rules,¹⁰ etc. In most of the cases listed, the Court of Justice of the European Union reviews various operations with personal data in the context of the protection of personal data (Directive 95/46/EC and the General Data Protection Regulation) and the Charter of Fundamental Rights of the European Union, in particular in the context of Article 7 (“Respect for private and family life”) and Article 8 (“Protection of personal data”).

However, as mentioned above, the fact that the legislative act provides for the storage or disclosure of personal data from state administrative databases and interferes with a person’s private life does not necessarily mean, in the practice of the Constitutional Court, that this legislation ultimately restricts the individual’s fundamental rights and, consequently, the provision is considered incompatible with the right to private life. In order to assess the restriction of the right or freedom, the Constitutional Court (2018-18-01, pt. 16; 2022-09-01, pt. 12) examines whether the restriction is (1) provided for by law; (2) justified by a legitimate aim; and (3) proportionate.

Furthermore, in order to assess the proportionality of the restriction of fundamental rights, it must be established whether (1) the chosen measures

¹ *OT v. Vyriausioji tarnybinės etikos komisija* [2022].

² *WM and Sovim SA v. Luxembourg Business Registers* [2022].

³ *Ligue des droits humains ASBL v. Conseil des ministres* [2022].

⁴ *Peter Puškár v. Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy* [2017].

⁵ *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni* [2017].

⁶ *W. P. Willems and Others v. Burgemeester van Nuth and Others* [2015]; *Michael Schwarz v. Stadt Bochum* [2013].

⁷ *Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others* [2015].

⁸ *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen* [2010].

⁹ *Latvijas Republikas Saeima (Points de pénalité)* [2021].

¹⁰ *SO v. Nationale Anti-Doping Agentur Austria GmbH (NADA) and Others* [2023].

are suitable for achieving the legitimate aim; (2) there are means less restrictive (mitigating) of the fundamental rights of individuals; and (3) the benefit gained by society exceeds the damage caused to the rights and lawful interests of individuals (Constitutional Court, 2018-18-01, pt. 19; 2022-09-01, pt. 16).

In both cases, the Constitutional Court ruled that the restrictions were provided for by law and justified by a legitimate aim, but were not proportionate.

5. Error of the legislator in assessing the proportionality of the restriction

In the first case concerning demerit points, the Constitutional Court accepted that the legitimate aim of the measure was to protect the public and the rights of others. In fact, the disclosure of information on demerit points provides more information on violations (driving discipline) and thus has the potential, in some cases, to reduce the participation in road traffic of persons who regularly violate road traffic rules. This may promote compliance with road traffic rules and increase road safety. (Constitutional Court, 2018-18-01, pt. 20) However, the Constitutional Court found that the legislator, by providing for the information to be generally accessible and thus disclosed to anyone (including persons who do not need it to ensure and promote road traffic safety), provided for a too wide and unconditional circle of possible recipients, given the purpose of the contested legal norms. In fact, according to the Constitutional Court, there were less restrictive measures (less restrictive of fundamental rights): if the information on the registered demerit points of a particular person were to have the status of “information with restricted access,” those persons (companies, or private individuals) who actually need this information could obtain it anyway by other means, but on the other hand, adequate guarantees for the rights and freedoms of the data subject would be ensured. (Constitutional Court, 2018-18-01, pt. 21.1) Thus, given that, in this case, there were measures that were less restrictive of a person’s rights, the Constitutional Court ruled that the restriction of fundamental rights contained in the contested norm was incompatible with the principle of proportionality and Article 96 of the Constitution (Constitutional Court, 2018-18-01, pt. 21.2).

In the second case, concerning the storage of data of acquitted persons, the Constitutional Court accepted the legislator's argument that the legitimate aim of the provision was the "protection of the democratic state order, public security and the rights of others" (Constitutional Court, 2022-09-01, pt. 14.4). Namely, that the data stored in the archive database of the Punishment Register, specifically those of acquitted persons, could be used to decide on the reopening of criminal proceedings on the basis of newly discovered circumstances. Secondly, such data could also be used by the persons concerned as official confirmation of their acquittal and to claim compensation for the damage caused to them during the criminal proceedings (Constitutional Court, 2022-09-01, pts. 14.3, 14.4 & 17.2). However, the Constitutional Court ruled that these two objectives could be achieved by measures that were less restrictive of a person. The Court noted that it is not necessary to keep data on acquittals for a lifetime, since the renewal of criminal proceedings on the basis of newly discovered circumstances is limited by the shorter prescribed period (Constitutional Court, 2022-09-01, pt. 18). Additionally, as regards the assumption that the individual himself will need this data in the future, the Constitutional Court argued that this argument of the legislator cannot serve as a reason to store the data against the will of the individual, since the individual has the right to not exercise his rights. In the absence of any other legitimate purpose for keeping the data, the state has no reason to store a significant amount of personal data on the pretext that it may be useful to the individual at some point in the future (Constitutional Court, 2022-09-01, pt. 18). Thus, the Court held that the additional duplication and storage of the data of an acquitted person in the archive database for 100 years from the person's birth and for one year after the person's death was not necessary for the achievement of the legitimate objective (Constitutional Court, 2022-09-01, pt. 18) and that the provision was therefore incompatible with the right to respect for private life (Article 96 of the Constitution).

These two cases show that national legislation mandating the storage of personal data in public administrative databases may be insufficiently considered by the legislator and may thus jeopardise fundamental rights, in particular the right to respect for private life. The Achilles' heel in these two cases was the consideration of the proportionality test.

If personal data must be stored in public administrative databases at all, the legislator must be aware that the storage of personal data in public administrative databases interferes with a person's private life, and therefore the legislator must comprehensively consider whether the restriction is

proportionate, including whether there are measures that would be less restrictive of a person's rights and would allow the legitimate aim to be achieved in the same quality.

6. Lessons for legislators in establishing future administrative databases

The methodology in these two cases presents that, depending on the context, a legislative measure may fail to be proportional if, for example, the information available in a state administrative database:

- 1) is stored longer than it is necessary for the aim of the data storage itself (Constitutional Court, 2022-09-01, pt. 18);
- 2) is too widely and unconditionally available to the public (has the status of “generally accessible information”), even though there are measures available that would be less restrictive upon a person's rights to respect for private life.¹¹

However, drawing inspiration from the system of the European Human Rights Convention or the Charter of Fundamental Rights of the European Union, the list of issues that may cause problems with regard to the proportionality test can be extended with other examples of case-law, such as:

- 1) Storing personal data (such as fingerprints) in a database of persons suspected of having committed a criminal offence, but who are not ultimately convicted (e.g., *M.K. v. France* [2013]; cf. *S. and Marper v. The United Kingdom* [2008]);
- 2) Retaining personal data that indirectly discloses special categories of personal data (such as the indefinite retention of personal data from peaceful public protests revealing the political opinions of the individual (e.g., *Catt v. The United Kingdom* [2019]) or the online publication of name-specific data relating to the data subject's spouse, partner, or cohabitant are likely to reveal information about the private life of the data subject, including, for example, their sexual orientation) (e.g., *OT v. Vyriausioji tarnybinės etikos komisija* [2022]);

¹¹ Also, *WM and Sovim SA v. Luxembourg Business Registers* [2022], in relation to access for any member of the general public to the information on beneficial ownership (a register of beneficial ownership).

- 3) Imposing a fixed period for the retention of genetic data (e.g., DNA) samples from convicted offenders, irrespective of the seriousness of the offence and without the possibility of requesting their destruction (*Aycaguer v. France* [2017]);
- 4) Disclosing criminal records from databases to prospective employers to the extent that it may have a significant impact on the employment prospects of the data subject (disclosure without distinction as to the seriousness or circumstances of the offence) (*M.M. v. The United Kingdom* [2012]; cf. *Sõro v. Estonia* [2015]);
- 5) Failing to take sufficiently into account the range of public authorities having access to the database and/or to establish clear rules on confidentiality and clearly defined circumstances under which the database can be consulted (*Gardel v. France* [2009]);
- 6) Failing to prevent the legislation on recording or rectifying personal data in the database creates insurmountable barriers for someone who wishes to change it (for example, to change categories of personal data such as an ethnic identity different from that recorded in respect of one's parents (*Ciubotaru v. Moldova* [2010]), religion (*Sinan Işık v. Turkey* [2010]), or gender (*Christine Goodwin v. The United Kingdom* [2002]));
- 7) Continuing to retain the nature and age of the information not supported by reasons which are relevant and sufficient as regards the protection of national security (*Segerstedt-Wiberg and Others v. Sweden* [2006]);
- 8) Using unacceptable form of publication of personal data: closed database versus a table that is accessible to the public online (*SO v. Nationale Anti-Doping Agentur Austria GmbH (NADA) and Others* [2023]).

In conclusion, personal data published in state administrative databases must be based on external regulatory enactments (laws), which serve to guarantee the protection of private life.

However, the two cases analysed in this article and the complementary jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union reveal that national legislation mandating the storage of personal data in state administrative databases may be insufficiently considered by legislators and, as a result, may jeopardise fundamental rights. The author concludes that the Achilles' heel in these cases has usually been the consideration of the proportionality test.

When personal data must be stored in public administrative databases, the legislator must be aware that the storage of personal data in public

administrative databases interferes with a person's private life, and therefore the legislator must fully assess whether measures that would be less restrictive of a person's rights exist and allow the legitimate aim to be achieved with the same quality. Enlisted case-law examples present various expressions of proportionality.

Aleksandrs Potaičuks, PhD is an assistant professor (docent) at Riga Graduate School of Law. He defended his PhD at the University of Latvia in 2020 in the field of recognition of foreign administrative acts. Currently, Dr. Potaičuks specialises in administrative law and European Union law. Previously, he was a Judicial Counsellor at the Supreme Court of Latvia and the Constitutional Court of Latvia.

References

- Aycaguer v. France* [2017], ECtHR Application no. 8806/12, 22.6.2017. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-175007> [accessed 29 May 2024]
- Bar-Siman-Tov, I.** (2012), 'Semiprocedural Judicial Review,' *Legisprudence*, vol. 6, no. 3, pp. 271–300. <https://doi.org/10.5235/17521467.6.3.271>
- Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni* [2017], CJEU Case C-398/15, ECLI:EU:C:2017:197, 9.3.2017.
- Catt v. The United Kingdom* [2013], ECtHR Application no. 43514/15, 24.1.2019. Retrieved from <https://hudoc.echr.coe.int/fre?i=001-189424> [accessed 29 May 2024]
- Charter of Fundamental Rights of the European Union, *OJ C* 326, 26.10.2012.
- Christine Goodwin v. The United Kingdom* [2002], ECtHR Application no. 28957/95, 11.7. 2002. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-65153> [accessed Aug 2024]
- Ciubotaru v. Moldova* [2010], ECtHR Application no. 27138/04, 17.4.2010. Retrieved from <https://hudoc.echr.coe.int/fre?i=001-98445> [accessed 29 May 2024]
- Constitutional Court of Latvia, Case no. 2018-18-01 of November 13, 2021, *Latvijas Vēstnesis* 223, 16.11.2021.
- Constitutional Court of Latvia, Case no. 2022-09-01 of December 22, 2022, *Latvijas Vēstnesis* 250, 27.12.2022.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 'On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,' *OJ L* 281, 23.11.1995.

- Gardel v. France* [2009], ECtHR Application no. 16428/05, 17.12.2009. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-96457> [accessed 29 May 2024]
- Gaughran v. The United Kingdom* [2020], ECtHR Application no. 45245/15, 13.2.2020. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-200817> [accessed 29 May 2024]
- Hofmann, H.; Schneider, J. P. & Ziller, J.**, eds. (2014), *ReNEUAL Model Rules on EU Administrative Procedure*, ReNEUAL Research Network on EU Administrative Law.
- Latvijas Republikas Saeima (Points de pénalité)* [2021], CJEU Case C-439/19, ECLI:EU:C:2021:504, 22.6.2021.
- Law on Road Traffic, *Latvijas Vēstnesis* 274/276, 1.10.1997.
- Law on State Information Systems, *Latvijas Vēstnesis* 76, 2.5.2002.
- Ligue des droits humains ASBL v. Conseil des ministres* [2022], CJEU Case C-817/19, ECLI:EU:C:2022:491, 21.6.2022.
- Michael Schwarz v. Stadt Bochum* [2013], CJEU Case C-291/12, ECLI:EU:C:2013:670, 17.10.2013.
- M.K. v. France* [2013], ECtHR Application no. 19522/09, 18.4.2013. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-119075> [accessed 29 May 2024]
- M.M. v. the United Kingdom* [2012], ECtHR Application no. 24029/07, 13.11.2012. Retrieved from <https://hudoc.echr.coe.int/fre?i=001-114517> [accessed 29 May 2024]
- OT v. Vyriausioji tarnybinės etikos komisija* [2022], CJEU Case C-184/20, ECLI:EU:C:2022:601, 1.8.2022.
- Peter Puškár v. Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy* [2017], CJEU Case C-73/16, ECLI:EU:C:2017:725, 27.9.2017.
- Pleps, J.; Pastars, E. & Plakane, I.** (2022), *Constitutional Law*, Rīga: Latvijas Vēstnesis. Retrieved from https://juristavards.lv/wwwraksti/JV/BIBLIOTEKA/GRAMATAS/KT_ENG.PDF [accessed 29 May 2024]
- Punishment Register Law, *Latvijas Vēstnesis* 211, 10.10.2013.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, *OJ L* 119/1, 4.5.2016.
- S. and Marper v. the United Kingdom* [2008], ECtHR Application no. 30562/04, 4.12.2008. Retrieved from <https://hudoc.echr.coe.int/fre?i=001-90051> [accessed 29 May 2024]
- Sarat, A.; Douglas, L. & Umphrey, M. M.**, eds. (2012), *Imagining New Legalities: Privacy and Its Possibilities in the 21st Century*, Stanford: Stanford University Press.
- Segerstedt-Wiberg and Others v. Sweden* [2006], ECtHR Application no. 62332/00, 6.6.2006. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-75591> [accessed 29 May 2024]

- Shimovolos v. Russia* [2011], European Court of Human Rights Application no. 30194/09, 21.6.2011 (28.11.2011 final). Retrieved from <https://hudoc.echr.coe.int/eng?i=001-105217> [accessed 29 May 2024]
- Sinan Işık v. Turkey* [2010], ECtHR Application no. 21924/05, 2.2. 2010. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-97087> [accessed 29 May 2024]
- Smaranda Bara and Others v. Casa Națională de Asigurări de Sănătate and Others* [2015], CJEU Case C-201/14, ECLI:EU:C:2015:638, 1.10.2015.
- SO v. Nationale Anti-Doping Agentur Austria GmbH (NADA) and Others* [2023], CJEU Case C-115/22, ECLI:EU:C:2023:676, 14.9.2023.
- Sõro v. Estonia* [2015], ECtHR Application no. 22588/08, 3.9.2015. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-156518> [accessed 29 May 2024]
- Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen* [2010], CJEU Joined Cases C-92/09 and C-93/09, ECLI:EU:C:2010:662, 9.11.2010.
- WM and Sovim SA v. Luxembourg Business Registers* [2022], CJEU Joined Cases C-37/20 and C-601/20, ECLI:EU:C:2022:912, 22.11.2022.
- W. P. Willems and Others v. Burgemeester van Nuth and Others* [2015], CJEU Case C-446/12, ECLI:EU:C:2015:238, 16.4.2015.