Eneken Tikk

Magister iuris, Adjunct Lecturer, University of Tartu

Monika Mikiver

LL.M., Head of the Department of Public Law, Public Service Academy

Applicability of the Census Case in Estonian Personal Data Protection Law

Estonian personal data protection law tends to adopt the German doctrine of informational self-determination as delivered by the *Bundesverfassungsgericht* (BVerfG) in its 1983 census ruling. While the new fundamental right deriving from this landmark case has influenced personal data protection law widely all over Europe, the authors take a critical look at national prerequisites for applying the principles deriving from the 1983 case. The elements of the census case are of a dynamic nature and cannot be applied without deeper analysis of the facts and context of the case, thereby calling for a systematic interpretation of its outcome.

The aim of this article is to provide an analytical structure for determining the correspondence of the principles and conclusions of the census case to Estonian information law. The proposed structure of the analysis can be used also as a basis for relevant analysis in other countries within the EU data protection law framework.[*1]

1. Reasons for questioning the Estonian doctrine

One modern way to achieve a better democracy is to establish additional guarantees to free movement of information. Today, virtually all Member States of The European Union (EU) have adopted laws on access to public-sector information.

[1] The basis for national regulation of personal data protection in the member states, and thereby another important source of interpretation in the field, is Directive 95/46/EC (i.e. Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995, on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ L 281, 23.11.1995, p. 31). Still, the solutions provided to problems of protection of private life differ by country. While Hungary has balanced the two fundamental rights in a single act, in the Czech Republic the subject of the data is entitled to the widest of powers in relation to the data processors and Sweden has preserved a remarkable margin of publication.

Estonia, in enacting its Public Information Act[*2] (PIA), was among the first countries in Europe to offer a general instrument granting access to public-sector information. The act sets forth decisive steps toward securing the transparency of public-sector activities — by, e.g., requiring all Estonian state and local authorities to maintain a Web site and make accessible to the public any information that has been received or created in the course of carrying out public activities.

In its more than five years of application, the PIA has shown several practical problems and occasioned theoretical quandaries, most of these related to the issue of coherent application of the PIA concurrently with the Personal Data Protection Act[*3] (PDPA).[*4] The conflict of the two acts is fundamental: while the PDPA is aimed at securing the privacy of individuals, the PIA sees as its main goal the transparency of the exercising authority. Against the background of the different direction of these laws, the ideal of a transparent society made up of non-transparent individuals is difficult to achieve.

No official commentaries and best practice have yet been issued by Estonian authorities regarding the mutual application of the conflicting rights contained in the PDPA and PIA. Therefore, the comments to the Constitution, relevant court rulings, and decisions of supervisory authorities are a very valuable asset in determining the nature of the country's personal data protection regime and the basic approaches necessary for advising clients and proposing new regulatory steps in this environment.[*5]

The first commentary to the Constitution of the Republic of Estonia, published 10 years after its enactment in 1992, takes the view that the right of a person to informational self-determination should be established upon the foundation of the German archetype expressed in the *Volkszählungsurteil*[*6] of the German Constitutional Court.[*7] The same view has gradually been taken up by the Estonian legal chancellor[*8], the Data Protection Inspectorate[*9], and several Estonian legal scientists.

In view of the fact that the PDPA was drafted on the basis of German and Finnish legislation[*10], the use and application of German court practice to prepare and interpret Estonian legal acts in the field deserves independent analysis and reasoning.

2. The census case

The key elements of the census case may be summarised as follows:

- under the conditions of modern data processing shall be guaranteed the right of every person to decide how much information is to be disclosed about him or her, and when, and
- limitations to this right are tolerable only in cases of clear and overwhelming public interest and with the legal basis of a well-defined purpose.

[2] Avaliku teabe seadus. – Riigi Teataja (State Gazette) I 2000, 92, 597 (in Estonian). English text available at http://www.legaltext.ee/ (1.05.2006).

[3] Isikuandmete kaitse seadus. – Riigi Teataja (State Gazette) I 1996, 48, 944 (in Estonian). Reformed in 2003, Riigi Teataja (State Gazette) 2003, 26, 158. English text available at http://www.legaltext.ee/ (1.06.2006).

[4] For more detail, see E. Tikk, M. Mikiver. Informatsioonilise enesemääramise õigusetagamise diskretsiooniotsused haldusmenetluses (Discretional Decisions of Guaranteering the Right of Informational Self-determination). – Juridica 2005/4, pp. 250–258 (in Estonian).

[5] Recently, the Estonian Ministry of Social Affairs commenced a public procurement proceeding for creating the legal environment for the launch of the Estonian electronic health information system in 2008. The initial analysis conducted by the offerents shows that varying modifications to personal data protection acts have been adopted in EU member states. For further information, see http://www.sm.ee/ (1.06.2006).

[6] BVerfG 15.12.1983. In BVerfGE 65, 1 et seq., EuGRZ 1983, 577: Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83.

[7] M. Ernits. – Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne (Constitution of the Republic of Estonia. Commented Edition). Tallinn: Juura 2002, p. 213 et seq. (in Estonian).

[8] Õiguskantsleri 2004. a tegevuse ülevaade (Overview of the Activities of the Chancellor of Justice in 2004), pp. 183–195, text available (in Estonian) at http://www.oiguskantsler.ee/.files/12.pdf (1.06.2006); Õiguskantsleri 2003–2004. a tegevuse ülevaade (Overview of the Activities of the Chancellor of Justice in 2003–2004), pp. 41–43, 159–168, text available (in Estonian) at http://www.oiguskantsler.ee/.files/11.pdf (1.06.2006); Õiguskantsleri 2002. a tegevuse ülevaade (Overview of the Activities of the Chancellor of Justice in 2002), pp. 65–66 (in Estonian), available at http://www.oiguskantsler.ee/.files/2002.pdf (1.06.2006).

[9] See the reports published at http://www.dp.gov.ee/ (1.06.2006).

[10] Explanatory letter to the PDPA. Available at http://web.riigikogu.ee/ems/saros-bin/mgetdoc?itemid=022900017&login=proov&password=&system=ems&server=ragne11 (1.06.2006) (in Estonian).

2.1. Facts and background on the case

In 1982, the West-German Bundestag unanimously enacted a census law (*Volkszählungsgesetz*[*11]) whereby personal data (given name and surname, phone number, sex, birthday, marital status, citizenship, and fact of having or not having a religious affiliation) gathered during the census may be compared to data included in national registries (*Melderegistern*), with the latter to be corrected on the basis of such data.[*12] Anonymous data referred to above, as well as a significant quantity of other data (including income, participation in acquisitions, data about domicile, etc.), were allowed to be transmitted to competent public and local authorities for purposes of their carrying out their mandates.[*13]

The main aims of the law on the census were to enable updating of the information from that of the previous census, carried out in 1970, about the population in the federation and at state and local administrative division level and to guarantee the quality of decision-making related to, e.g., space planning and the labour market, as well as social, education, and traffic policy.[*14] After the law was enacted, many complaints were filed with the BVerfG. The reason for anxiety among these people was the fear of potential threats likely to be caused by computerised processing of their data.[*15]

Proceedings on constitutional supervision were initiated, and on 15 December 1983 the BVerfG declared § 9 (1)–(3) of the act null and void, thereby evidencing great concern about individuals' **privacy in relation to the position of a person in the feared autocratic state**.[*16] The ruling stated that the guarantees of human dignity[*17] and the right to free self-actualisation[*18] create the basis for protection of a person against unconstrained processing of personal data, stating also that limitations to such protection are tolerable only in cases of **prevailing public interest**.[*19]

2.2. The right to informational self-determination

2.2.1. The basis of articles 2 (1) and 1 (1) of the German Constitution

The BVerfG sets forth the principle that the individual has the right to know what information is being processed that pertains to him or her and to make decisions on the basis thereof.[*20] The court argued that "the freedom of an individual to decide for himself is at stake when the individual is uncertain about what is known about him, particularly where what society might view as deviant behaviour is at stake. The individual therefore has the right to know and make decisions on the information being processed about him".[*21]

---

[11] Das Gesetz über eine Volkszählung, Berufszählung, Wohnungszlählung und Arbeitsstättenzählung vom 25. März 1982. – BGBl I p. 369.

[12] Section 2 of the German Census Act: "Die Volkszählung und Berufszählung erfaßt: 1. Vornamen und Familiennamen, Anschrift, Telefonanschluß, Geschlecht, Geburtstag, Familienstand, rechtliche Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft, Staatsangehörigkeit; 2. Nutzung der Wohnung als alleinige Wohnung, Hauptwohnung oder Nebenwohnung (§ 12 Abs. 2 des Melderechtsrahmengesetzes). § 9 (1): Angaben der Volkszählung nach § 2 Nr. 1 und 2 können mit den Melderegistern verglichen und zu deren Berichtigung verwendet werden. Aus diesen Angaben gewonnene Erkenntnisse dürfen nicht zu Maßnahmen gegen den einzelnen Auskunftspflichtigen verwendet werden."

[13] See § 9 (2) of the German Census Act: "Einzelangaben ohne Namen über die nach den §§ 2 bis 4 erfassten Tatbestände dürfen nach § 11 Abs. 3 des Bundesstatistikgesetzes vom 14. März 1980 (BGBl I S 289) von den Statistischen Ämtern des Bundes und der Länder an die fachlich zuständigen obersten Bundesbehörden und Landesbehörden übermittelt werden, soweit sie zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich sind. § 9 (3): Für Zwecke der Regionalplanung, des Vermessungswesens, der gemeindlichen Planung und des Umweltschutzes dürfen den Gemeinden und Gemeindeverbänden die erforderlichen Einzelangaben ohne Namen über die nach den §§ 2 bis 4 mit Ausnahme des Merkmals rechtliche Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft in § 2 Nr. 1 sowie der nach § 4 Nr. 1 Buchstabe c und § 4 Nr. 3 Buchstabe c erfassten Tatbestände der Auskunftspflichtigen ihres Zuständigkeitsbereiches von den Statistischen Ämtern der Länder übermittelt werden."

[14] BVerfG as in Note 6 *supra*, p. 13.

[15] "Die Möglichkeiten der modernen Datenverarbeitung sind weithin nur noch für Fachleute durchschaubar und können beim Staatsbürger die Furcht vor einer unkontrollierbaren Persönlichkeitsfassung selbst dann auslösen, wenn der Gesetzgeber lediglich solche Angaben verlangt, die erforderlich und zumutbar sind," in BVerfG as cited in Note 6, p. 2.

[16] See, e.g., L. Young. Among the Giants. New York 1966.

[17] GG § 1 (2): "Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

[18] GG § 2 (2): "Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

[19] BVerfG as in Note 6 *supra*, remark 156.

[20] *Ibid*., remark 155: "Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

[21] *Ibid*., remark 23.

The ruling derived the right of informational self-determination — the right of a person to decide how much information to allow to be disclosed about him or her, and when[*22] — from the **principle of human dignity** enshrined in articles 2 (1) and 1 (1) of the German Constitution. The court has ruled that the guarantees to human dignity[*23] and the right to free development of one's personality[*24] create the basis for protection of a person against unconstrained processing of personal data.

However, the right to informational self-determination shall not be granted without limits. The court has stated that limitations to such protection are tolerable, although only where there is a prevailing public interest.[*25]

2.2.2. The basis of the Estonian Constitution

Ernits is of the opinion that the general right to development of one's personality derives from § 19[*26] of the Estonian Constitution, covering the right to self-determination (which also comprises the right to informational self-determination).[*27] The latter, in Ernits's view, is the right of the individual to decide whether, and to what extent, data pertaining to him or her may be gathered and saved.[*28]

The Estonian legal chancellor predicates that the data processing can refer mainly to the right of privacy set forth in § 26 of the Estonian Constitution but that in some situations the right of informational self-determination devolves from § 19.[*29]

Pursuant to § 19 (2), everyone is obliged to honour and consider the rights and freedoms of others, as well as to observe the law both in exercising his or her rights and freedoms and in carrying out his or her duties.

2.3. The reasoning of the court

According to the BVerfG, an important prerequisite to individual self-determination is the opportunity of an individual to first freely decide upon a behaviour, and then the guarantee of the chosen behaviour to be effected.[*30]

The BVerfG analysis reflects the concern about individual **privacy in relation to the person in relationship to the feared autocratic state**.[*31] Unlike before, there are now new threats in the form of possibilities of using the personal data in database in short order every time and from everywhere without regard for remoteness. By combining the information with that in order databases, it can be possible to create a full profile of a person, without the individual concerned having a chance to control the use and appropriateness of the information.[*32]

The above-mentioned analysis states: "It is […] relevant that the doctrine of informational self-determination when developed under national law takes into account the social, economic, legal, and other realities and secures an individual's right to act in his or her best interests and best determine his or her **informational situation** in a society. Through correct positioning in a society, one can with sufficient certainty rely on the action chosen and thereby gain the greatest benefit from the right to informational self-determination as thereby going beyond the pure right to privacy. Therefore, relevant is not only that the person's right to determine when processing is allowed should be guaranteed but also that the conditions of interference with such rights should be clearly determined."[*33]

If one cannot with sufficient certainty be aware of what personal information about him or her is known in a certain part of his social environment, (s)he can be seriously inhibited in his or her freedom of self-deter-

[22] BVerfG II 1) a: "aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart warden."

[23] GG § 1 (1): "Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt."

[24] GG § 2 (2): "Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

[25] BVerfG as in Note 6 *supra*, remark 156.

[26] Subsection 19 (1) of the Estonian Constitution provides the right to free self-determination.

[27] M. Ernits (Note 7), pp. 160–161.

[28] *Ibid*., p. 161.

[29] Õiguskantsleri 2004. a tegevuse ülevaade (Note 8), p. 46.

[30] See reports cited in Note 9 *supra*, remark 1.

[31] See, e.g., L. Young (Note 16).

[32] BVerfG as cited in Note 6 *supra*, p. 22.

[33] H. Lisken, E. Denninger (eds.). Handbuch des Polizeirechts. Munich: C. H. Beck 1996, p. 610, marginal note 8.

mined planning and decision. A society in which individual citizens could not find out who knows what and when about them would not be reconcilable with the right of self-determination over personal data. Those who are unsure whether differing attitudes and actions are ubiquitously noted and permanently stored, processed, or distributed will try not to stand out in their behaviour. This would not only limit the opportunities for individual development but also affect the public welfare, since self-determination is an essential requirement for a democratic society that is built on the participatory powers of its citizens.[*34]

However, the right to informational self-determination has its limits. As noted above, the court stated that limitations to protection of the right to personal self-determination are tolerable in cases of prevailing public interest.[*35]

2.4. Transformation of the case

The influences of *Volkszählungsurteil* are phenomenal: the case has influenced legal doctrines broadly and been cited by the Italians[*36], Swiss[*37], Hungarians[*38], Australians[*39], Americans[*40], and many others[*41], According to Roßnagel, the ruling about legal bases with defined purpose as a necessary condition for limitations of the right of self-determination was misunderstood. The BVerfG wanted to guarantee a higher lever of protection of personal data through the obligation of preventive control by legislative acts. A. Roßnagel wrote: "The consequence was a deluge of very fine and specific regulations in almost every branch, which are comprehensible only by data protection experts."[*42]

3. Obstacles to direct application of the census case under Estonian law

We next analyse the key elements of the census case in the Estonian context by arguing that:

- the relations involved in processing of personal data are increasingly private in nature, such that the applicability of the state–individual context needs to be assessed;
- the nature of the right of a person to informational self-determination in the information society has a different character; and
- there are less burdensome methods for achieving the control of the data subject over the processing of personal data than deciding about each and every event of processing.

[34] BVerfGE Volkszählungsurteil, p. 22.

[35] BVerfGE Volkszählungsurteil, p. 23: "Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbarer Herrschaft über "seine" Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. [...] Das Grundgesetz hat, wie in der Rechtsprechung der Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der Gemeinsch aftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden [...]."

[36] G. Sartor. Privacy, Reputation, and Trust: Some Implications for Data Protection. Information on this working paper is available at http://www.google.com/search?q=informational+self-determination+census&hl=et&lr=&start=30&sa=N (1.01.2006).

[37] M. Langheinrich. The Success of E-commerce May Hinge on a Fundamental Human Right …. Available at http://www.ipc.on.ca/docs/04-11-08-COASTSoftware.ppt (1.01.2006).

[38] C. D. Raab. Information Rights in Hungary: Observations on Experience. The Door onto the Other Side 2001.

[39] D. Lindsay. Misunderstanding "Personal Information": Durant v Financial Services Authority. – Privacy Law and Policy Reporter 2004 (13).

[40] C. H. Manny. Personal Privacy — Transatlantic Perspectives: European and American Privacy. Commerce, Rights and Justice. Part 1. – Computer Law and Security Report 2003 (19) 1.

[41] Available at http://en.wikipedia.org/wiki/Informational_Self-Determination (1.01.2006).

[42] "Das inhaltliche Ziel, die Verarbeitung personenbezogener Daten auf die wirklich unabdingbaren Fälle einzuschränken, wurde weitgehend verfehlt. Der Gesetzgeber hat dem politischen Druck der jeweiligen Verarbeitungswünsche nicht zu widerstehen vermocht – wenn er dies überhaupt wollte. Das Programm des Volkszählungsurteils wurde in einer Weise "erfüllt", die geradezu das Gegenteil von dem hervorbrachte, was beabsichtigt war. Statt normenklarer, auch für den Bürger verständlicher Gesetze, haben wir heute ein Datenschutzrecht, das insgesamt überreguliert, zersplittert und unübersichtlich ist," according to A. Roßnagel. '20 Jahre Volkszählungsurtreil'. – MultiMediaRecht (MMR) 2003, Heft 11, p. 694.

3.1. Scope of application of the reasoning in private and public processing

3.1.1. Undefined area of privacy

There are different dimensions of privacy recognised and protected in legal terms: Most authors distinguish among physical, psychological, social, and informational dimensions of privacy. The latter is often referred to as the 'umbrella term' for data protection and informational self-determination.

In an earlier German case, often cited as 'Microcensus'[*43], the German court had stressed that the guarantee to an inviolable sphere of privacy beyond the reach of public authority is rooted in article 1 of the *Grundgesetz*. In the Microcensus case, the court established that there are three spheres of human personality, only two of which are to be protected under the right to privacy:

- a social sphere containing information concerning open social interaction with other persons (*Sozialsphäre*),
- a private sphere related to information concerning private life without being usually accessible to the public (*Privatsphäre*), and
- a personal sphere concerning private life and relating to information that is confidential and secret from the individual's point of view (*Intimsphäre*).

The distinction among the different spheres of personality was not addressed specifically in the census case. In essence, the court abandoned the distinction between the spheres and delineated the scope of the right.

It is, therefore, open to question whether the conclusions of the census case are to be applied to all spheres of privacy or only the social one.

3.1.2. Undefined area of processing

According to the prevailing point of view, the right to privacy was first established as a right of an individual to protection against the state.[*44] The ruling also outlawed the non-proportional interest of the state where personal data are concerned.

Nowadays, a great danger to informational self-determination arises from private-sector processing — for purposes of banking, insurance, medical and other supply services, communication, etc., thousands of pieces of personal data are processed daily. Often these data are combined by undertakings to better serve their customers' interests.

According to Steven Hetcher, the norms that have emerged in private processing are more efficient and respectful to personal privacy than the existing public-law concept is.[*45] Hetcher has also concluded that respect for privacy does not require minimising the amount of personal data processing, his view providing a contrast against the perception evident in much national legislation.[*46] In practical relations concerning data protection in the private sector, data subjects have often stressed that the more data the processor has about them, the more qualified services and products are offered to them, which is regarded as a benefit by many consumers.[*47]

As the fundamental rights primarily concern the relationship between the individual and the state[*48], one should ask, in the context of private data processing taking over a role that was that of the state, how, if at all, the doctrine is to be applied to processing of personal data by private entities.

Shortly after the ruling was made by the BVerfG, Costas Simitis noted that the principles established in the case of the census are to be applied to processing of personal data under private law.[*49] Articles 2 I i. V and

[43] BVerfG 27, 1, 16.07.1969.

[44] As to the background, see, e.g., S. Singleton. Privacy and Human Rights: Comparing the United States to Europe, at http://www.cato.org/pub_display.php?pub_id=5082) (1.01.2006). The horrors of the Holocaust inspired many Europeans to give renewed attention to the problem of privacy in the years following World War II. National-Socialist-style governments in several countries used national census data to identify households of certain ethnic, religious, or other targeted groups. In the United States, at around the same time, census information was used to identify Japanese-Americans for relocation.

[45] S. A. Hetcher. The Emergence of Website Privacy Norms. – Michigan Telecommunications Law Review 2001 (7) 1, pp. 12–29.

[46] Data protection principles may be characterised by the key word 'rationality'. However, customer surveys indicate that customers are satisfied with offers actually fulfilling their expectations.

[47] Seen the final conclusions of the Seminar on Data Protection in the Private Sector, held in Tallinn, 23.11.2003.

[48] M. Ernits (Note 7), p. 162.

[49] S. Simitis. Revisiting Sensitive Data. – Neue Juristische Wochenschrift (NJW) 1984, p. 401.

1 I of the *Grundgesetz* are the basis for *Drittwirkung* theory under German law, and Simitis derives an overall obligation from the census ruling.*[50]

Hence, shortly thereafter, J. Wente refers to the *herrschende Lehre* and state law by concluding that no absolute *Drittwirkung* can be applied to fundamental rights. The dominant school bases its reasoning on that of Ernst Dürig.*[51]

Using the doctrine of horizontal effects, one may come to the conclusion that the right to informational privacy*[52] no longer exists only in public law but has been extended also to private relations. Yet legal scholars support the view that it is too narrow to regard privacy as a relationship between the individual and the state.*[53]

The application of absolute *Drittwirkung* theory would lead to a situation where also relationships in private law depend on the margin of the entitlement of the state. To avoid such a situation, the content of *Drittwirkung* is to be interpreted and modified, which in turn can lead to arbitrary conclusions.*[54]

Therefore, it is important to differentiate between private and public events of personal data processing, as the census case addresses only the latter.

3.2. Alternative solutions to modern problems

"Restricting information about himself and his emotions is a crucial way of protecting the individual in the stresses and strains of [...] social interaction", Alan Westin says, supporting the reasoning of BVerfG.*[55] Informational privacy is lost when information about a person is obtained against his or her will, be it because there is an obligation to disclose it or because it concerns an area of intimacy over which the individual wishes to retain control.

Yet, if privacy depends only on personal control over it, one has no significant privacy and never will in a computerised world.*[56] Several authors have argued that the factor of control has a different meaning and scope in the modern data processing context. Indeed, today control on the part of the individual is guaranteed by means of consent, the right to access and correct the data, and the right to withdraw consent and be informed about processing of data gathered from third parties.

Also, exercising constant informed control about all uses of personal data may be burdensome, given that most personal data are processed by automatic means. Several events of processing are necessary solely for purposes of enabling individuals to use services that they have requested. In this situation, the rigid concept of control often overrides interests such as comfort of activities or speed of transactions.

3.3. Different public and different interest

To illustrate the fundamental differences of the concepts of 'public' and 'interest' as referred to by the court from those obtaining in Estonia 23 years later, we next take a look at some public services successfully implemented by the Estonian authorities.

Since 2001, Estonians have had the opportunity to declare their taxes online. One third of the Estonian population carry out their banking activities online, and around 50% use the Internet in the course of their daily activities. In the census ruling, the court expressed a fear of unfamiliar technical opportunities allowing the uncontrollable spread of personal data to different databases.*[57]

---

[50] Stated thus: "Die informationelle Selbstbestimmung überall dort zu respektieren, wo personenbezogene Daten verarbeitet werden."

[51] J. Wente. Informationelles Selbstbestimmungsrecht und absolute Drittwirkung der Grundrechte. – Neue Juristische Wochenschrift 1984, Part 25, p. 1446: Danach enthalten Grundrechte in ihren objektiv-rechtlichen Gewährleistungen Wertentscheidungen, die über Art. 1 III GG auf die gesamte Rechtsordnung ausstrahlen und Gesetzgebung, Rechtsprechung und Verwaltung binden.

[52] The term 'informational privacy' as used by A. F. Westin, J. Gafo, and others can be regarded as, in essence, synonymous to 'informational self-determination'. This is seen in, e.g., Westin's "informational privacy relates to an individual's right to determine how, when and to what extent data about the self will be released to another person". See works such as his Privacy and Freedom. London: Bodley Head 1967, with the quoted text appearing on p. 25.

[53] P. Blume. Nordic Data Protection. Helsinki: Kauppakaari Oyj 2001, p. 6.

[54] See Westin's Privacy and Freedom as cited in Note 52 *supra*.

[55] *Ibid*., p. 13.

[56] H. T. Tavani, J. H. Moor. Privacy Protection, Control of Information and Privacy-enhancing Technologies. – Computers and Society 2001 (31) 1, pp. 7–11.

[57] See reports cited in Note 9 *supra*, remark 22.

The pilot project of the 'e-police' uses the feature of checking the identity, driver's licence details, and validity of the automotive insurance policy of Estonian drivers online. All Estonian insurance companies therefore provide the police with information about the motor insurance.

In assessing whether it is necessary to apply the double standard of control that derives from the census case, one should first determine whether other interests — such as economy of activities, general freedom of information, and freedom of expression — must be considered.

3.4. Leads for interpretation in the census case

In its argumentation in the census case the court stressed that the scope of protection and the concept of human dignity are to be considered in the context of **modern** developments and **new** threats to one's personality[*58], stating that "this right requires a special level of protection under contemporary and future circumstances of automated data processing".

The need for legal protection of the autonomy of an individual in deciding whether, when, and under what circumstances to reveal facts about him- or herself was stressed by Westin a decade and a half earlier, and by Warren and Brandeis almost a hundred years before. The threats addressed by the high court, jurists in academia, and privacy advocates always have been related to 'contemporary' challenges, which in Warren and Brandeis's case was the spread of information via photography in the media, for Westin the opportunity to tap telephone conversations and track human activities with surveillance cameras, and for the BVerfG automated data processing in its rather trivial form.[*59]

After two decades, the reality of data processing has dramatically changed in terms of both quality and quantity: information is processed mainly through automated processes, and the quantity of data readily accessible to anyone has increased dramatically.

It is unsurprising that, in an application of common sense, the development of information technology can be, and has been, put into the service of better protection of personal data — e.g., in the introduction of regulations allowing officials to access information systems only in a traceable and controllable manner. Various preventive measures and means of control create a reason to reassess the fears addressed by the court. The PDPA *expressis verbis* states the principle of data security and specifies the measures to be taken by processors to ensure it.

Today, most EU member states differentiate between sensitive and non-sensitive personal data.

4. Conclusions and proposed structure of analysis

Though data protection laws traditionally form the core of the legal area of informational self-determination[*60], there are significant areas of developments in the scope of informational privacy, among them the freedom of expression and information.

In order to decide whether the reasoning of the census case may be applied under national law, one must address the following questions:

- Is the legal relationship in question public (as opposed to private) in nature?
- Is the case directed at the dignity and personality of the individual concerned?
- Is it possible to achieve the aims of personal data protection in a manner less restrictive than prohibition of data processing?
- Is there a public interest involved that is likely to outweigh the privacy of the individual concerned, and how is the concept of public interest defined under national law?

[58] *Ibid*., remark 1.

[59] *Ibid*., II 1) a: Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entschei-dungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten (vgl § 2 Abs. 1 BDSG)) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind.

[60] G. Robbers. Informationelle Selbstbsetimmung und allgemenine Informationsfreiheit in Deutschland. – Juridica International 2002 (VII), pp. 98–105.

It is difficult to overestimate the valuable input of the German Constitutional Court for the development of privacy law. Yet, applying the reasoning of the high court in a transforming and non-selective manner leads to the development of personal data protection law into a mutated entity that is something wholly different.

According to Marie-Theres Tinnefeld, the original aim of the court can be achieved only through simplifying the law on data protection and making it more understandable.[*61] In order for this to be done, changes in society and technology must be taken into account.

[61] M.-T. Tinnefeld. Die Novellierung des BDSG im Zeichen des Gemeinschaftsrechts. – NJW 2001, p. 3079; A. Roßnagel. 20 Jahre Volkszählungsurtreil. – MMR 2003, 11, p. 694.