READER

„The German Bible of Data Protection"

(Constitutional Courts Census Act)

and other ressources, helping to being active in understanding, saving and restoring privacy in times of more and more digitalized daily life

Special edition, designed for the European Commission, DG Home,
regarding future stand on Data Retention

Personal Issue for Mr. ...

Edited and handed out by the people of freiheitsfoo
16 October 2015

Content

1. Census Act (Extract)

English translation of essential parts of the German “Volkszählungsurteil” from 15 December 1983, which established in Germany the Basic Right on Informational Self-Determination.

Complete Text: http://freiheitsfoo.de/census-act/

Headnotes

1.
Given the context of modern data processing, the protection of individuals against unlimited collection, storage, use and transfer of their personal data is subsumed under the general right of personality governed by Article 2.1 in conjunction with Article 1.1 of the German Basic Law (Grundgesetz - GG). In that regard, this fundamental right guarantees in principle the power of individuals to make their own decisions as regards the disclosure and use of their personal data.

2.
Restrictions of this right to "informational self-determination" are permissible only in case of an overriding general public interest. Such restrictions must have a constitutional basis that satisfies the requirement of legal certainty in keeping with the rule of law. The legislature must ensure that its statutory regulations respect the principle of proportionality. The legislature must also make provision for organizational and procedural precautions that preclude the threat of violation of the right of personality.

3.
As regards the Constitutional requirements to be satisfied by such restrictions, it is necessary to distinguish between personal data that are collected and processed in personalized, non-anonymous form and data intended for statistical purposes.
In the case of data collected for statistical purposes, it is not possible to require the existence of a narrowly defined, concrete purpose for the collection of such data. However, the collection and processing of information must be accompanied by appropriate restrictions within the information system to compensate for the absence of such a concrete purpose.

4.
The survey program of the 1983 Census Act (Volkszählungsgesetz - VZG) does not entail registration and classification of personal data that would he incompatible with human dignity; it therefore also satisfies the requirements of legal certainty and proportionality. Nonetheless, procedural precautions are required in connection with the execution and organisation of the collection of such data in order to preserve the right to informational self-determination.

5.
The provisions governing the transfer of data (including for the purposes of crosschecks with population registers) contained in s. 9.1 to 3 of the 1983 Census Act violate the general right of personality. The transfer of data for scientific purposes is compatible with the Basic Law.

Important Notes of the Court

The worth and dignity of individuals, who through free self-determination function as members of a free society, lie at the core of the constitutional order. In addition to specific guarantees of freedom, the general right of personal]ty guaranteed m Article 2.1 in conjunction with Article 1.1 of the Basic Law, which can also become important precisely in view of modern developments and the concomitant new threats to the personality, serves to protect that worth and dignity. Previous concrete treatment in the case law does not conclusively describe the content of the right of personality. This right also subsumes - as has already been suggested in the BVerfGE 54, 148 decision in extension of previous decisions. - the right of individuals that follows from this idea of self-determination to decide in principle themselves when and within what limits personal matters are disclosed.

Given the current and future state of automated data processing, this right merits a special measure of protection. It is especially threatened since it is no longer necessary to consult manually assembled flies and dossiers for the purposes of decision making processes, as was the case previously; to the contrary, it is today technically possible, with the help of automated data processing to store indefinitely and retrieve at any time, in a matter of seconds and without regard to distance, specific information on the personal or material circumstances of individuals whose identity is known or can be ascertained (personal data (see s. 2.1 of the Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG)). This information can also be combined - especially if integrated information systems are set up - with other collections of data to assemble a partial or essentially complete personality profile without giving the party affected an adequate opportunity to control the accuracy or the use

of that profile. As a result, the possibilities for consultation and manipulation have expanded to a previously unknown extent, which can affect the conduct of the individual because of the mere psychological pressure of public access.

However, personal self-determination also presupposes - even in the context of modern information processing technologies - that individuals are to be afforded the freedom to decide whether to engage in or desist from certain activities, including the possibility of actually conducting themselves in accordance with their decisions. The freedom of individuals to make plans or decisions in reliance on their personal powers of self-determination may be significantly inhibited if they cannot with sufficient certainty determine what information on them is known in certain areas of their social sphere and in some measure appraise the extent of knowledge in the possession of possible interlocutors. A social order in which individuals can no longer ascertain who knows what about them and when and a legal order that makes this possible would not be compatible with the right to informational self-determination. A person who is uncertain as to whether unusual behaviour is being taken note of at all times and the information permanently stored, used or transferred to others will attempt to avoid Standing out through such behaviour. Persons who assume, for example, that attendance of an assembly or participation in a citizens' interest group will be officially recorded and that this could expose them to risks will possibly waive exercise of their corresponding fundamental rights (Articles 8 and 9 of the Basic Law). This would not only restrict the possibilities for personal development of those individuals but also be detrimental to the public good since self-determination is an elementary prerequisite for the functioning of a free democratic society predicated on the freedom of action and participation of its members.

From this follows that free development of personality presupposes, in the context of modern data processing, protection of individuals against the unrestricted collection, storage, use and transfer of their personal data. This protection is therefore subsumed under the fundamental right contained in Article 2.1 in conjunction with Article 1.1 of the Basic Law. In that regard, the fundamental right guarantees in principle the power of individuals to make their own decisions as regards the disclosure and use of their personal data.

(...)

The use of the data is limited to the purpose specified by law. If for no other reason than because of the dangers associated with automated data processing, protection is required against unauthorized use - including protection against such use by other governmental entities - through a prohibition on the transfer and use of such data. Mandatory information, disclosure and deletion constitute further procedural precautions

2. Microcensus Case (Extract)

Extract from the "Microcensus Case", Source: German Constitutional Court from 16 July 1969, Order BVerfGE 27, 1, Margin numbers 32-34

Complete Text: https://wiki.freiheitsfoo.de/pmwiki.php?n=Main.Microcensus-Case

According to the Basic Law's set of values, human dignity is of paramount importance. As is the case for all provisions of the Basic Law, this affirmation of human dignity also governs Art. 2 sec. 1 GG. The state cannot through any measure, not even a law, violate human dignity or otherwise interfere with the freedom of the person in its essence, beyond the limits drawn in Art. 2 sec. 1 GG. Thus, the Basic Law confers on each individual citizen an inviolable sphere of private life choices that is beyond the influence of public authority.

In the light of this concept of the human being, all human beings living in a community enjoy a right to social value and recognition. It would violate human dignity to make a human being a mere object within the state. It would be incompatible with human dignity if the state were to claim the right to compulsorily register and catalogue a human being in his or her entire personality, even under the anonymity of a statistical survey, and thereby to treat one as a commodity, accessible for inventory in every respect.

The government is interdicted to undertake such intrusion into privacy via comprehensive inspection of the personal circumstances of its citizens because for a free and responsible development of his personality sake the individual must remain an interior in which he

has himself and in which he can retreat and where the environment has no access, in which one is left alone and enjoys a right to solitude, a right to reclusiveness. This protected area can already possibly be harmed by government engaged inspection, which is able to inhibit the free development of personality through the psychological pressure of public involvement - even if the valuation might be ment neutral.

3. European Court of Justice: Data Retention (Extract)

Judgement of the Cour of Justice (Grand Chamber) about EU Data Retention Direcitve, 8 April 2014, In Joined Cases C-293/12 and C-594/12, Margin numbers 37, 51-52 and 58-59

Complete Text: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1

It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

(...)

As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a

retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.

(...)

Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

4. European Court of Justice: Safe Harbour (Extract)

Judgement of the Cour of Justice (Grand Chamber) about Safe Harbour, 6 October 2015, In Case C-362/14, Margin numbers 93-94

Source: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362

Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).

In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by

Article 7 of the Charter (see, to this effect, judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39).

5. Letter from freiheitsfoo to Mr. Avramopoulos from 3 Nov 2014 (Extract)

Extract of the first letter from german NGO „freiheitsfoo“ to Mr. Avramopoulos, becoming part of a longer mailconversation.

Complete Sources: https://wiki.freiheitsfoo.de/pmwiki.php?n=Main.20141103Brief-an-Avramopoulos#toc7

You stated perfectly correct that the European Court of Justice considered Data Retention as disproportionate and invalid. It is also true that the judgment couldn't in principle exclude a possible relevance of investigation technique to guarantee public safety. Therefore to conclude a modified europeanwide Data Retention Directive without any cause as a response within the meaning of the judgment is quite simply wrong.

The European Court of Justice's judgement didn't criticise single elements of Data Retention Directive, but voiced fundamental critique of saving telecommunications data throughout Europe. Whereas, it underlined the great significance of the fundamental right of privacy and stressed the necessity to protect personal data.

To clarify our position, we kindly ask you to study the manageably extensive paragraphs 31, 51, 52, 58 and 59 of the European Court of Justice's judgement. The Court therein clearly points out its statements and conclusions. Concerning the outstanding issues of how effectivly controlling information technology systems, we in addition mark paragraph 55 that limits/stops Data Retention in its previous form.

With this in mind, to reissue a modified europeanwide Data Retention Directive with the aim of saving geographically and temporally indefinite datas may not be your concern. Rather, as European Commissioner of Migration and Home Affairs it would be your responsibility and duty to remedy the fault caused by (and in substantially shared responsibility of EU Commission) the previous EU Directive on Data Retention violative of human rights: Persons in the European Union need to be protected against a europeanwide collection and retention of telecommunications data without cause. This will only be possible if you ensure the abolition of Data retention already implemented or continued in many EU Member States. Data Retention must be banned - that's your job, Mr. Avramopoulos!

Imprint
www.freiheitsfoo.de