DNA, THE ULTIMATE PERSONAL DATA, IS VISUALIZED IN THE CBP-LOGO

The desire...

The desire to use increasing amounts of personal data for a growing number of purposes is the prominent issue in many social debates. Without pretending to come even close to a complete picture, the discussion about intensifying the combating of terrorism, the introduction of the citizen's personal identity number and the drastic change to the health insurance system to incorporate market forces can serve as examples. We must also mention the desire to arrive at more intensive exchange of information between different institutions and organisations that increasingly try to realise an interconnecting client system, for the fulfilment of a public task or otherwise. Private enterprises are required to make data about commercial transactions available for government purposes and customer data are shared within conglomerates as sources of information. Technological breakthroughs or the mass application of existing technology open the door to previously unheard-of ways for monitoring, analysing and assessing the actions of individuals and for treating them according to the information compiled. Thus, the field supervised by the Dutch DPA is currently changing drastically.

Needless to say, tension arises in balancing the desire or perceived need for 'invading' someone's privacy on the one hand and the statutory requirements for the careful handling of personal data on the other hand. In order to bring this 'battle' to a productive synthesis the cooperation of the government, the private sector and the Dutch DPA is needed. Those in the public and private sector who wish to realise innovations or changes should – more so than is currently the case in most instances – realise the principles of the protection of personal privacy in order to use them to find solutions for possible dilemmas. For the Dutch Data Protection Authority (DPA), on the other hand, the rule applies that it is intensely aware – or should be aware – of new social developments and needs.

The framework within which the Dutch DPA then acts is, to a large extent, restricted by the relevant statutory stipulations and the instruction to be derived from these stipulations, whereby the Personal Data Protection Act (WBP) – more so than a number of other laws – determines the actions of the regulatory authority. The history of the realisation of the WBP, and the developments since then, provide us with complex dilemmas in this respect.

As ever, if the legislator resorts to codification of that which has grown in everyday practice or which is deemed to be desirable as a standard in a political-social sense, over the course of time attention focuses more on the technical implementation of the law than on the matter to be protected or the objective to be realised which is hidden behind this technical implementation. In these cases the application of the law looks mostly formalistic, while the material interest is hidden from view. In other words: in the eyes of some parties the Dutch DPA is an 'administrative burden' rather than the 'privacy watchdog'.

It also strikes me as curious that the fundamental right in question was ultimately converted into national legislation on the basis of a European Directive that aims to combat unfair competition. More so than the protection of the citizen, it appears the protection of the consumer was the driving force to arrive at this specific form of codification. This is even more surprising because, in cases in which the statutory stipulations are considered too restrictive for the sector-specific objectives to be realised, the central government can introduce new legislation that can still make it possible for the requirements the WBP imposes on the way personal data is handled to be met. The WBP therefore appears to have a considerably less binding character in the public sector than in the private sector.

In the public debate there has, for some years, been a strong erosion and politicisation of the term 'privacy'. The action radius of the Dutch DPA is determined by the concretely described instruction in the WBP to make a contribution to the protection of personal data. This is generally referred to as privacy protection. In the social debate the term 'privacy' is also used in a casual sense without even a remote stipulation as to what this refers to. In recent years 'privacy' has, for many people, also become a political 'bone of contention': a vaguely defined interest that supposedly prevents administrators and professionals from realising politically and socially desirable objectives. In statements from politicians, administrators and other officials – for

instance the now traditional far-reaching New Year's addresses of Chiefs of Police – criticism of 'privacy' as an obstacle to action and as a hiding place for defaulters, fraudsters and other malicious persons has become a recurring cover for the lack of decisiveness or successful action on the part of organisation in question.

What is irritating about these statements is the fact that they are never or hardly ever accompanied by examples to demonstrate exactly what the problem is. Insofar as concrete situations are given as examples that are supposed to show that the WBP (or any other statutory stipulation that provides for the protection of personal data) actually obstructs the realisation of politically or socially desirable objectives it usually becomes clear on closer consideration that there was in fact unprofessional conduct on the part of the party complaining about the obstacle, or – sometimes very – limited knowledge of the possibilities the Act most certainly does provide.

What was and is the essence of what the WBP is supposed to protect? And how must this protection be realised? The Dutch Constitution, the European Convention on Human Rights, the Strasbourg Data Convention and the draft Constitution for the European Union all document privacy protection and, consequently, the protection of personal data. The first value is the protection of personal privacy, guarantees against offensive or unwarranted intrusion into the life of citizens. The primary objective of this protection is to enable citizens to have a certain freedom of action.

To this effect all individuals want some level of control over what others know about them, about the image others have of them. Everyone is entitled to and has an interest in being able to determine, to a certain extent, if, and if so in which way, distribution of information that is generated or stored about him or her is to take place. From the point of view of the citizen and consumer the right of self-determination, autonomy and individual development – always to be relatively interpreted in a democratic state under the rule of law – are therefore the key values with respect to the norms and the resulting rules for dealing with personal data.

If power and the exercise of power are linked to personal data, an unjustifiable restriction of the social opportunities and development of the individual may result. The technical 'translation' into everyday social practice that has been made in the WBP means that citizens and consumers are entitled to and must be able to rely on the fact that the government and the private sector will deal with personal data in a decent, respectful and transparent manner.

The following chapters of the 2004 annual report list many concrete stated cases and recommendations in which the Dutch DPA, with due observance of the law, has tried to fulfil its task as a regulatory authority in a contemporary manner. The search for an acceptable balance between the seemingly conflicting interests of protecting personal data on the one hand and market, political or

social needs on the other is a recalcitrant one, as this report shows. It is a legitimate question – and one that must be asked frequently – whether any single stipulation in the WBP hinders us rather than helps us in this search.

An intensification of the search for an acceptable balance is advisable, both for the Dutch DPA and for 'those responsible'– the government and private parties – and, if possible, one that is based on reciprocity. After all, trust between people and organisations in society is, in part, determined by the way personal privacy is respected and more specifically the way in which personal data is handled. Can the individual 'look over the shoulder' and determine if, and if so what, information is being circulated about him or her? In what way have checks and balances been implemented so that effective control of the collection, processing and sharing of personal data is possible?

Ultimately, finding a good balance benefits the way in which individuals are able to give their trust to society. A society that is able to generate this social capital for its citizens has created an important boundary condition for prosperity and well-being, for a blossoming civil society, for a society that finds strength and safety in cohesion.

J. Kohnstamm
chairman