Access, protection of privacy and archives : trends in the electronic age

Autor(en): **Olsen, Poul Erik**

Objekttyp: **Article**

Zeitschrift: **Traverse : Zeitschrift für Geschichte = Revue d'histoire**

Band (Jahr): **10 (2003)**

Heft 2

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-24355

ACCESS, PROTECTION OF PRIVACY, AND ARCHIVES

TRENDS IN THE ELECTRONIC AGE

POUL ERIK OLSEN

I shall be honoured in trying to give an overview of one of the challenges the archivists – and I may say, very many others – are facing in the electronic age. It has to do with classical archival questions about access. Questions about access have traditionally and rightly been topics of debate. Now, in the electronic age, they are even more so. The overview falls in three parts. First, I shall examine the impacts of new technology on the legislation on secrecy and openness. Second, I shall try to give an overview of the concept of privacy and of legislation concerning the protection of privacy, and finally I shall try to hint what the implications of the tensions between openness and privacy may be for archives.

SECRECY AND OPENNESS: THE IMPACTS OF TECHNOLOGY

Archives contain a lot of records – we all know that. And we know something more: We hold our records with the purpose of making them accessible for our guests in our readings rooms, be they researchers, writers, journalists or just quite ordinary people who come to seek information about the history of the society in which they live. We know that we cannot grant access to some of our records that hold information pertaining to the security of the state, to defence, or foreign policy matters, etc. Access is here limited so as to protect the security of our states, of our public organizations. The problem that I shall deal with the question of access to records containing information of individual persons. But we might remind ourselves that both issues have to do with the same set of problems of secrecy and openness, which are properties of normal social interaction. For the individual as well as for the organization or the state, it seems to be a prerequisite of social interaction to be able to choose what to keep secret and what not. The lack of ability to make this choice will make social interaction virtually impossible. The absence of secrecy makes individuality and personal identity impossible to achieve, excessive secrecy will cut

off the individual from social interaction. For the state or the organization, excessive secrecy may diminish the ability to readjust to outside changes, hinder communication and internal decisionmaking. Lack of secrecy, on the other hand creates a vulnerability to external forces that may endanger the very existence of the organization.

In the course of history, states have been very secretive about their affairs. It was normally considered that the state had a right to be secretive, while on the other hand the citizens of a state should have no secrets – at least not from the state. For the last five decades, the trend has been rather the reverse: One the one hand, we have *Transparency of Government,* that is that the state should have no – or as few as possible – secrets from its citizen, and on the other *Protection of Privacy,* that is that the citizens have a right to keep private matters secret, even from the state. And if the citizen should share his private secrets with the state, the state will have to ensure that nobody else learns them.

Freedom of Information can be defined as the right to seek and receive information. This definition, at least, is in accordance with the interpretation of the Declaration of Human Rights. In an archival connection, however, it should be noted that the right to receive information, as statuted by the Declaration, does not encompass freedom of information in the sense that public authorities are obliged to give information at the request of the citizen. In what degree public authorities are so obliged, has not been regulated in international or supranational law, although in many national laws, until the coming into force October 24, 1998, of the *Directive 95/46/EC of the European Union,* which is concerned with data protection. It is yet to be seen if the directive will have a comprehensive impact on not only the data protection legislation of the European states, but also on the Freedom of Information or Open Government legislations.

The different national legislations of Freedom of Information, Open Government, etc. and also the archival legislation of some countries regulate the rights of citizens to access to public documents. As a rule, exceptions or limitations from a general right to access to public documents are based on the security or interest of the state, but also on the interest of its individual citizens or other third parties.

You could sum up that Freedom of Information legislation or legislation on access has to do with the assumption that the state should have no secrecy, whereas data protection legislation deals with the citizens having a right to secrecy. As an example of the tension between these two assumption I can quote the *Freedom of Information and Protection of Privacy Act of British Columbia* in Canada, where it says that the basic goals of the act arc "to make public bodies more accountable to the public and to protect privacy". If these goals come into conflict, which to put first?

To give a sweeping statement, in the *Freedom of Information Acts* of the paper age, personal data could be withheld from public access, but to be so they should qualify by being sensitive, that is to say they should contain information whose disclosure might injure privacy – trivial information would not be kept secret. In more recent legislation and practice, the tension between data protection legislation and Freedom of Information laws has become greater. That has to do with the revolution in technology. 50 years ago – in a paper environment – it was still a cumbersome job to collect and process information about individuals; the limited search and copying capabilities afforded data subjects with a degree of privacy protection. Decisions about public access that were made when information was stored on paper did not reflect any growing concern about privacy issues because of the difficulties involved in using the records. In the age of the mainframe the dangers to privacy from public use also was limited, but the exchange of personal data between government agencies (or other mainframe users) was seen as the primary privacy problem. Data matching became the primary target of legislation. Roughly stated, public access regulations were based on the same assumptions as in the paper environment. With the coming of the powerful personal computer and the Internet, it is suddenly easy beyond belief both to collect, copy, store, communicate, process, and reprocess personal data.

As Gregory Rawlins has put it: "We all swim in an invisible sea of secrets. Visit a bank and you create a file, go to the doctor and you create a file; log on to a computer and you create a file." Almost any everyday activity of an individual leads to that information about that individual is gathered, stored, and processed. And in a manner, that allows for the effective use of that information. Of course, it is beyond doubt that there are very great advantages connected to the use of modern information technology. For instance, it makes it possible for everyone, including archives, to store incredible amounts of information in very little space. The technology makes it very easy to find in the masses of the data the information you need and to communicate that information to others. But neither can it be doubted that the technology contains an inherent risk that the privacy of individuals might be injured. The more sophisticated the technology becomes, the greater are the risks of misuse. Thus, one effect of the evolution of information technology is that protection of the privacy of physic persons has taken a still higher place on the political agenda, but on the other hand the technological capabilities has left administrators and legislators rather speechless. For instance, the rapid development of the Internet has taken legislators by surprise – and it is now virtually impossible to control its development by legislation.

THE CONCEPT OF PRIVACY

Historically, the "big brother"-syndrome has played a very big role in the data protection ideology and has placed data protection among the human right issues. Indeed, the same year that George Orwell's "1984" was published the *Universal Declaration of Human Rights* was formulated. Its Article 12 states: "No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has a right to the protection of the law against such interferences or attacks."
We have here the right to privacy defined as one of the fundamental human rights. Rules that states that the right to privacy should be protected can also be found in constitutions or fundamental law of nearly all nations. Most penal codes stipulates punishment for injuries to privacy etc. And this is not a new phenomenon. Some will argue that legislation about privacy can be traced back till l4th century England. Another historical example that is often mentioned is the *Swedish Public Records Act* of 1766. But what should be protected? What means privacy?
The argument starts at the point where the need for a definition of "privacy" arises; there is no commonly agreed description or definition of "privacy". Danish jurist Peter Blume has remarked that you do not know what privacy is until you have lost it and it is too late to regain it. This ties nicely into the discussion above. The definition of privacy and the definition of secrecy dependent on its social and cultural context. In the case of that specialty of protection of privacy that is constituted by data protection, very often reference is made to the description of Samuel Warren & Louis Brandeis in 1890. Warren & Brandeis assumed that a person has a right to be left alone and a right to self-determination with respect to disclosures of private matters or informational selfdetermination. The assumption is that an individual person possesses a private domain and that it is he or she that decides whether others can have access to this domain – in other words that the person whom data concern has the ownership to these data. Data form part of the Roman Law persona, of the integrity of the individual. In its extreme, it will follow from the latter part of this definition that everything that can be connected to an individual is private or personal data. For instance the *French Data Protection Law* defines information to be personal where "in any form whatsoever, it allows natural persons to be identified by it, directly or otherwise". The same goes for the *Directive of the European Union.* Sometimes it is argued that not all personal data are subject to protection of privacy. Social interaction demands that some minimum of information cannot be regarded as secret or private. Outside of the domain of privacy may fall trivial information, but even information that in

one connection is clearly trivial, can in other connections be private. For instance address information is normally considered trivial; however if this information reveals that an individual is residing in a psychiatric hospital as a patient, it may be private.

There has been a trend in legislation to identify various types of personal data as trivial, sensitive or very sensitive, and there is much commonality in the lists of sensitive data in national data protection legislations. For example, political views, criminal records and religious and sexual preferations are usually listed as sensitive or very sensitive data. On should be aware, however, that the topics listed are as unclear as the definition of privacy itself and that they cover areas that are difficult to delimit. Also, the interpretation of sensitive data may vary from country to country or even inside the same country: In the USA for example, the US Supreme Court decided in 1994 that the socalled rap sheet (centralized records on individual's criminal convictions, held by the FBI) is protected by the privacy legislation, but in the state of Ohio it is public information. That is to say, that the same information might in one context fall under the protection of privacy and in another not. The US Supreme Court based its verdict on a archival/technological basis: "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, country archives, and local police stations throughout the country and in a computerized summary located in a single clearinghouse of information." If we adhere to the abstract assumption that privacy deals with the protection of the individual against infringements of his or her personal integrity, regardless of how the personal integrity is injured, it can be a little difficult to understand that vast difference. Does it mean that the amount of work that has to be put into invading the privacy of an individual can justify the invasion? Or is it simply a matter of "paper" versus "electronic" privacy? It is probably the last. The line between trivial and sensitive information can thus only be drawn in abstract terms. A definition of sensitive data could be data whose disclosure may threaten the privacy or personal integrity of an individual, although the information in itself does not qualify as particularly sensitive or confidential. Also to be taken into account might be the degree of accessability. The topics under which a particular set of data may fall, cannot in itself determine whether data concerning an individual should be regarded as sensitive or not. Rather, the sensitivity of data is determined by the connection in which the data is processed or used. Data, which in one context may be trivial, becomes sensitive when used in other context or linked or matched with other (trivial) data. This would mean that some information that has hitherto been public socalled public registers – might have to be made secret or at least not readily accessible. An example is the *American Driver's Privacy Protection*

Act from 1994. Before the Act, registers of drivers' licenses were open to the public, but after an incident of misuse of the public information a law was passed making the registers inaccessible. In Norway, tax information is still accessible to the public, but the issue is debated; in France, voters registers are open, in Denmark, property registers are public, etc. Data protection legislation may here come into conflict with the tradition of some countries to keep public registers, and thus lead to limitation of the free access to public registers by broadening the concept of privacy. One could take this as an example of how the concept of privacy varies over time, in different social contexts, or in different technological settings.

THE MEANS OF PROTECTION

Data protection legislation concerns itself with the protection of personal data, i. e. that the goal of the legislation is the protection of privacy. Multinational or supranational organization has – either from human rights perspective or from economic – that is to say: transborder data flow – perspectives published guidelines for data protection legislation. One can mention i. a. the *United Nations Guidelines concerning Computerized Personal Data* for 14 December 1990 or the *Guidelines of the OECD* from 23 September 1980. The Guidelines contain a number of principles, i. a. lawfulness and fairness, accuracy, purpose-specification, interested-person access, non-discrimination, security, supervision. These principles form the common denominator of national data protections legislation. They can maybe be reduced to three fundamental principles transparency, consent, finalité. Transparency includes that an individual that are subject to the processing of personal data should be informed by the processing authority or the data controller that data is being processed, of the purpose of the processing, etc. Consent will mean that the object of a (future) registration or data processing should give his/her consent before data can be gathered or processed and in some cases also give consent before data is made available to third parties. Finalité prohibition of secondary use means that personal data which have been collected for a specific purpose should be used for that purpose alone and not for any other purpose. It will be seen that these principles or concepts lead to a legislation that puts the stress on procedures. It sets up legal standards that will have to be filled out and made more exact in practice.

From the viewpoint of protection of privacy, there can be little argument that the principles of transparency, consent and finalité should be adhered to. The arguments against the complete implementation of these principles are usually

based on grounds of economic rationality or administrative or technological expediency. The finalité principle is constantly under pressure because it forms a restriction on the use of data processing technology. Arguments against full adherence to the principle of transparency are based on economy. For instance, the cost of informing each individual that data about him or her is being processed can be very high for the controller. To aquire consent of the individual can also be very costly or a least be viewed as bureaucratic and impractical. From the principles you can conclude that the question of whether personal data is "owned" by the individual whom the data concerns, or they are the property of the data controller has more or less been resolved upon. The trend is – and in data protection legislation always has been – to define personal data not as "res in commercio", but as part of the persona. On this basis the newer data protection legislation gives the individual more extensive rights to control the use of personal data about him or her. The rights are guaranteed by the set of procedures that data controllers are legally bound to follow.

PUBLIC ARCHIVES AND PERSONAL DATA

As a rule, archival legislation is in comparison with data protection legislation relatively clear and simple. Common to all archival legislation is rules concerning the preservation of documents of historical and/or administrative or legal interest. It follows logically that documents preserved from reasons of historical interest should be accessible, and that access should be as wide as possible. In so far more recent documents are held in archival repositories, free access may be limited in consideration of public or private interests. How the limitations of free access are regulated, varies from country to country, from rules incorporated in archival law, to general laws on freedom of information, privacy laws. This does not in itself present problems with regard to the access to personal data, as long as it is agreed that the obligations of public archives to protect privacy are the same or if anything greater than the obligations of other public agencies – certainly not smaller. But it cannot be overlooked that the tensions between archival law and data protection law can be greater than the tensions between data protection and freedom of information. If we go back to the reading room scenario, we shall remember that the records we hold should be accessible for any legitimate purpose of our readers or researchers, not just for specified purposes, as would follow from the finalité principle, combined with the assumption of data ownership. In some data protection laws – for instance the Danish – the transfer of computerized personal data to public archives is the exception rather than the rule. Preservation of computerized

personal data requires a dispensation from Data Inspection Agency. This rule is based on the finalité principle or the principle of prohibition of secondary use of personal data. In practice, however, dispensations have not been hard to get, even when the data can be defined as very sensitive, but the dispensations have usually been based on harsher limitations to free access than in the case of non-computerized personal data. That the finalité principle can pose a problem for the transfer of personal data to archives and to the use of personal data in future research is recognized in the *EU Directive 95/461EC,* where it is stated in article 6, 1, b) that "further processing of data for historical, statistical or scientific purposes shall not be considered incompatible [with the specified, explicit and legitimate purposes for which the data was originally collected] provided that the Member States provide appropriate guarantees". The appropriate guarantees may be linked to the general limitations to free access as mentioned above or to the general data protection regulations. Access to archival documents may however serve other purposes than historical – in its widest sense – research. For secondary use of personal data that cannot be defined as research, data protection legislation may prove to be a hindrance. Other problems related to the regulations of access to personal data are connected to the role of public archives as data controllers. In the case of the EU Directive, public archives to which personal data is transferred, will become data controllers and will in this capacity be obliged to follow the same regulations as other data controllers. Among other things, public archives will have the same obligations as other data controllers to provide information to data subjects or to give data subjects access to "their own" data. In view of masses of personal data transferred to and held by public archives the economical consequences of these obligations may be serious and in some cases prohibitive.

Traditional archival and freedom of information legislation has been based on the assumption that the state was the owner of the records produced by its authorities or agencies and that the state could dispose over the information contained in its records, f. i. by granting its citizens access to the information. The data ownership assumption in data protection legislation – if carried through consequently – can place limitations on the dispositions of the state in the field of archival access. Should archives be obliged to ensure the consent of a data subject before the transfer of personal data from an authority to the archives? Another problem could come up in connection with the principle of accuracy. Most data protection legislation stipulates that a data subject has the right to have inaccurate data erased and/or substituted with the correct up-to-date information. Non-actual data should in principle be erased. But is it not among the purposes of archives to preserve "non-actual", not-up-to-date

information? To document what has been instead of what is? Accuracy in historical information and in administrative information are two different things.

All this may sound pessimistic. That is, however, not my purpose. It has only been to point out some of the trends in the tensions that arise in fields where different principles come to clash. The first rule in such circumstances is then to keep one's eyes open. Archivist should be aware of and make themselves heard about the issues of protection of privacy and access. Archival matters – though I am sure that we all agree that they are of prime importance – are not always what lie foremost in the minds of legislators when they are dealing with matters that may have a bearing on archives – as data protection and other privacy issues. As an example of what we can do is to bring more transparency into the question of the long term, archival preservation of these personal data I have mentioned that in the *Data Protection Directive of the European Union* it is positively stipulated that personal data may be preserved for secondary uses – historical, statistical, or scientific – but it took hard work to get this short sentence in. If that had not happened, a number of European archives might have had to choose between breaking the law or doing away with central parts of their collections. And that was not what even the most hard-core data protectionists wanted. We have thus a special obligation as a profession to do our bit to ensure that the unwanted will not happen. In recent archival and data protection legislation there are examples of how a balance between the seemingly conflicting principles of the two might be struck. And from the diversity of solutions we can draw the lesson that there is not necessarily just one right way to achieve that balance. It depends – like the concept of privacy – of the social, cultural and legal context.

ZUSAMMENFASSUNG

ZUGANG, SCHUTZ DER PRIVATSPHÄRE UND DIE ARCHIVE. TRENDS IM ELEKTRONISCHEN ZEITALTER

Der Artikel thematisiert den Einfluss neuer Technologien auf die Archivgesetzgebung und geht gleichzeitig der Frage nach, welche Auswirkungen die Spannungen zwischen dem Anspruch auf Offenheit und dem Anspruch auf Schutz der Privatsphäre für die Archive haben können. In einem ersten Teil zum Bereich Geheimhaltung und Offenlegung werden die unterschiedlichen Gesetzgebungen im Bereich *Freedom of Information* referiert. In einem zweiten

Teil zum Konzept der Geheimhaltung geht der Autor auf die Problematik ein, dass es weder einen konsensfähigen Definition von Privatsphäre gibt, noch genügend klar ist, welche Informationen oder Daten als sensibel zu gelten haben. Daran anschliessend folgen in einem dritten Teil über die Auswirkungen und Bedeutung von Schutzbestrebungen Betrachtungen zu den Spannungsfeldern, die sich aus dem Aufeinandertreffen der unterschiedlichen Prinzipien «Legalität und Fairness», «Sorgfalt und Zugangsregelungen», «Nichtdiskriminierung und Sicherheit» ergeben. Der letzte Teil widmet der Autor allgemeinen Überlegungen zu einer möglichen Strategie, um mit den künftigen Herausforderungen des elektronischen Zeitalters fertig zu werden. In diesem Zusammenhang plädiert er – mit Verweis auf die Relevanz von als sensibel eingeschätzten Daten für die historische und statistische Auswertung – für das Evaluieren verschiedener Lösungen, da es notwendigerweise nicht nur einen richtigen Weg aus dem Dilemma gebe.

(Übersetzung: Simone Chiquet)