UIC John Marshall Journal of Information Technology & Privacy Law

Volume 3
Issue 1 *Computer/Law Journal - 1981*

Article 7

1981

Institutions of Data Protection - An Attempt at a Functional Explanation of European National Data Protection Laws, 3 Computer L.J. 167 (1981)

Herbert Burkert

INSTITUTIONS OF DATA PROTECTION—AN ATTEMPT AT A FUNCTIONAL EXPLANATION OF EUROPEAN NATIONAL DATA PROTECTION LAWS[1]

by HERBERT BURKERT*

CONTENTS

1. This Article is based on material from a joint study performed for the European Commission by three European research institutes: Gesellschaft für Mathematik und Datenverarbeitung (GMD) (Bonn, Federal Republic of Germany), Institut de Recherche en Informatique et en Automatique (IRIA (presently INRIA)) (Paris, France), and National Computing Centre (NCC) (Manchester, England). The English edition of this study is published by NCC. *See* GMD, IRIA & NCC, DATA SECURITY AND CONFIDENTIALITY (1979).

* Institut für Datenverarbeitung im Rechtswesen (IDR) (Institute for Data Processing and Law) in der Gesellschaft für Mathematik und Datenberarbeitung (GMD)—Federal Republic of Germany.

Seven countries in Western Europe have enacted data protection laws.[2] Other countries contemplate legislation contained in reports or prepared by commissions.[3] International agreements also have been discussed and prepared.[4]

Although the United States was one of the first countries to enact data protection laws, many Americans today view European data

---

2. AUSTRIA: Federal Act of 18th October 1978 on the Protection of Personal Data (Data Protection Act), BGB1 for the Republic of Austria, 28.11.1979, at 193 (English translation: OECD document DSTI/ICCP/79.11/02); DENMARK: Private Registers Etc. Act No. 293, Public Authorities Registers Act No. 294, both of 8th June 1978 (English translation by the Danish Ministry of Justice: OECD document DSTI/ICCP/79.11/05); FRANCE: Act 78-17 of 6th January, [1978] J.O. 227 (English translation: OECD document DSTI/ICCP/79.11/08); FEDERAL REPUBLIC OF GERMANY: Act on Protection Against the Misuse of Personal Data in Data Processing, Federal Data Protection Act, Bundesdatenschutzgesetz (BDSG) of 27th January 1977 (English translation: OECD document DSTI/ICCP/79.11/01); LUXEMBOURG: Law of 31st March 1979 Regulating the Use of Personal Data in Information Systems, Memorial of the Grand Duche de Luxembourg A No. 29, 11.4.1979; NORWAY: Act of 9th June 1978 Relating to Personal Data Registers (English translation: OECD document DSTI/ICCP/79.11/14); SWEDEN: Data Act of 19th January 1977 (English translation by the Swedish Data Inspection Board: OECD document DSTI/ICCP/79.11/18). The English version of these data protection acts (except Luxembourg) have been collected in one source. *See* 2 AMERICAN FEDERATION OF INFORMATION PROCESSING SOCIETIES, TRANSBORDER DATA FLOWS (1979).

3. *See, e.g.*, BELGIUM: VANDERPOORTEN REP., Doc. 846, no. 1, 1975-1976 Senate Session (April 8, 1976); NETHERLANDS: KOOPMANS COMM., PRIVACY AND PERSONAL RECORDING (State Publishing Office, Gravenhage 1976), *and* GOVERNMENT COMM. ON THE PROTECTION OF PRIVACY VIS-A-VIS PERSONAL DATA SYSTEMS, DRAFT BILL OF PERSONAL DATA SYSTEMS (November 30, 1976), *reprinted in* Committee of Experts on Data Protection, Council of Europe, Information Doc. No. EXP/DATA PROT. (77) 2 (January 24, 1977) (unofficial translation); SPAIN: Preliminary Draft, Spanish Act on Data Protection (1976), *reprinted in* Committee of Experts on Data Protection, Council of Europe, Information Doc. No. EXP/DATA PROT. (76)5; UNITED KINGDOM: COMM. ON DATA PROTECTION, HOME OFFICE OF SEC'Y OF STATE, LINDOP REPORT, CMND. No. 7341 (1978) (hereinafter LINDOP REPORT).

4. The European Parliament has passed recommendations for harmonizing data protection on the EEC level. *See* REPORT ON THE PROTECTION OF THE RIGHTS OF THE INDIVIDUAL IN THE FACE OF TECHNICAL DEVELOPMENTS IN DATA PROCESSING, [1978-1979] EUR. PARL. DOC. (No. 100/79) (1979) (hereinafter PROTECTION REPORT). The Council of Europe's Convention is open to signature. *See* Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Europ. T.S. No. 108 (1981). The OECD has elaborated guidelines concerning the transborder flow of personal data. *See* OECD document C(80) 58 (final), *reprinted in Symposium on Transborder Data Flows and the Protection of Privacy*, INFORMATION, COMPUTER AND COMMUNICATIONS POLICY SERIES (ICCP/OECD 1979).

protection regulations with concern and even distrust.[5] There is growing concern that European regulations would be impractical, bureaucratic, and detrimental to the free flow of information, especially with the impact these regulations would have on transborder data flow. Leaving aside the particular problems of transborder data flow, one reason for American concern seems to be that European laws have some features that are unfamiliar to the American data protection approach. These features include the implementation of data protection agencies, the omnibus approach[6] and the recent inclusion of legal persons.[7] Americans assume that the growing number of data protection agencies is creating a data protection bureaucracy that will make it difficult to benefit from the positive consequences of informational technologies.

Since, however, every European country with data protection regulation has such an agency, a closer look at this European approach is worthwhile.[8] It may seem presumptuous to talk about "the" European approach, especially to those who daily have to deal with data protection questions in the European environment; its manifold differences almost constitute a new branch of comparative law.[9]

An overview that identifies the general aspects rather than the specifics of European regulations is necessary. A functional approach should provide such a cautious generalisation.[10] Rather than looking at specific regulations in detail, this approach identifies the services that data protection laws, intentionally or unintentionally, provide for society and the means by which this is achieved. A func-

---

5. *See, e.g.*, McGuire, *The Information Age: An Introduction to Transborder Data Flow*, 20 JURIMETRICS 1 (1979-80); Bigelow, *Transborder Data Flow Barriers, id.* at 8.

6. Seven American states, however, also use the omnibus approach. *See* THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY app. 1, at 2 (1977) [hereinafter cited as PPSC].

7. Austria, Denmark, Luxembourg, and Norway have included legal persons in their data protection legislation.

8. The installment of data protection institutions is not unfamiliar to the United States. Arkansas has the Information Practices Board, Minnesota uses the Commissioner's Office of the Department of Administration, Ohio has the Personal Information Control Board and the Department of Administrative Services, and Utah uses the Secretary of State's Office. *See* PPSC, *supra* note 6, app. 1, at 4; Lautsch, *Digest and Analysis of State Legislation Relating to Computer Technology*, 20 JURIMETRICS J. 201 (1979-80).

9. *See, e.g.*, Bing, *A Comparative Outline of Privacy Legislation*, 2 COMP. L.Y.B. 149 (1978).

10. Since all European data protection laws lack a precise definition of privacy, there was reason to assume that functions and procedures established by these laws were at least as important as definitional decision criteria. One report discusses this definitional dilemma. *See* LINDOP REPORT, *supra* note 3, at ¶ 2.01-2.04.

tional approach would then give a pattern of recognition so that the various elements of such laws can be located more easily. Privacy laws themselves, however, seem to be part of a far broader change in the concept of law and legislation. Such general changes, which seem to be caused by the growing impact of complex technologies, will be discussed in part I. A description of the mechanics of data protection laws will follow in part II. Part III will then look into the specific role of data protection agencies against this background. Since the functional approach tends to limit itself to describing how elements interact to achieve a certain performance level for a given system, part IV will attempt a broader evaluation. The evaluation will be limited to the following issues: (1) what are the functionally equivalent options to data protection agencies, *i.e.*, what kind of other mechanisms could provide at least similar services for societies facing informational technology; (2) what arguments actually have led to the "European" choice; and finally, (3) what may be the specific risks of this choice.

I. THE CONCEPT OF "TECHNOLOGY LAW"

Data protection laws can be seen as one answer to a particular group of problems caused by the development of informational technology.[11] Data protection regulations are thus part of a new type of regulations caused by technological changes. Such changes call for legislative processes that have two objectives:

- Society must adapt to technology to take advantage of the merits of technological change.
- Technology must be adapted to the basic values of society to ensure social coherence in a changing environment.

A regulatory mechanism must keep a proper balance between these two objectives in order to achieve both technological progress and a general acceptance of this progress.

Most data protection problems reflect "old" societal conflicts, mainly over distribution of power between, for example, the individual (or groups of individuals) and the state, between consumer and provider, or between employer and employee. The "new" technological element in these almost classic dualisms seems to pose problems of a kind that no longer can be dealt with sufficiently by existing traditional regulation of these relationships. This assumption is based partly on the observation of a new "language of power." The traditional conflicts now are put in terms of information handling, *i.e.*, access to information, distribution of information,

11. Other problems include changes in the structure of the labor market, international, economic, and cultural dependencies, and system vulnerability.

and capability to process information. Regulations thus have to adapt to this new language in order to be accepted as adequate and relevant conflict solutions.[12]

These new concepts also are based, however, on the strong practical impact of technology on traditional forms of information handling. Some observers even believe that this practical impact leads to qualitative changes in social relationships. For example, the right of access is one of the fundamental problems of data protection. Before the rise of automated data processing, these rights of access were discussed in terms of the particular relationship in which they occurred; patient/doctor, employer/employee, and so on. Traditionally, they were discussed in terms of professional ethics, business practises, contract law, and labor law. In the age of informational and communications technology the same access to information problems are discussed in terms of distribution of informational power, because informational technology has enlarged the dimensions of these relationships in terms of quantity, space, time, and participants. More information can be handled within these relationships in a shorter time, distance is almost irrelevant, and the number of participants can be increased easily. Those who argue for qualitative changes in handling access to information point to the possibility of using algorithms, which formerly had been too complex to use economically. This general increase in complexity has made it impossible to monitor these relationships sufficiently. This loss of orientation requires techniques that reduce complexity. One of these techniques is the "data protection" right of access now being carefully designed into the relevant information system.

The acceptability of conflict resolutions raises two questions:

- How can regulations adapt to change and still preserve basic, accepted values, or at least avoid drastic change?
- Do these regulations have to be laws?

Changes in informational technology are not the first technological changes the legal system has had to face. The demands of modern society already have led to a general change in the concept of law. Legislation had to become part of the adaptive processes caused by technological change so that social coherence could be maintained and society's survival guaranteed. The problem, however, is the difficulty in steering demands. The economic system as main regulator of technological progress tends to be difficult to influence, if such influence is desired at all. Also, the instruments of technology assess-

12. This is not only a "language" problem. The new language reflects new concepts of generating and distributing social power, which consequently need new concepts for checks and balances.

ment are being developed and refined still and are far from being perfected. As a result legislators have to regulate in an environment of uncertainty. These difficulties have led to new types of laws.

Type one, usually occurring in an area where there is some practical, technical experience, is called a "specific technology law." This type of law employs technical terms and may contain special measurement values to be achieved or not to be surpassed. Such laws may read like technical manuals and are open to change with technical progress. They usually are addressed to a small number of the community, usually technicians in charge of handling the regulated technology. Type two, usually occurring in an area where there is little practical, technical experience, is called a "general technology law." Such laws are addressed to anyone who might come into contact with the technology and they almost read like political programs.

Both types are, of course, "ideal types" identified here for heuristic reasons, but very often new legislation is a mixture of both types, *e.g.*, privacy legislation. Both types are not fundamental, minimal rules addressed to the whole community to be obeyed for an indeterminate period. Both types put legislators into a dilemma: whether the area is dynamic (type one) or underdeveloped (type two), there is a certain urge "to do something about it." Legislators cannot delay because many individuals fear that data processing technology will invade their privacy and violate other civil rights.

Legislative action is needed because only laws can sufficiently convince doubters that the technology should be accepted, and only laws can provide adequate compromises for social conflicts in democratic societies. It is, however, very often difficult to know what to do and what consequences a particular measure may have, so the legislator would prefer to learn rather than to legislate. Sensor mechanisms that watch the regulated area and give feedback to the legislator must be created in order to increase knowledge.

II. THE ROLE OF DATA PROTECTION LAWS

This new concept of law ("specific technology law" versus "general technology law") explains many of the striking features of privacy laws, *e.g.*, the astonishing combination of very general and very specific regulations (the latter mainly with regard to data security or procedural questions), the reluctance to define privacy as such, the tendency to have specific regulations (for specific sectors of application, *e.g.*, health records) in addition to general rules, and the expressed intent to review the law regularly and to learn from the developments. Privacy laws thus can be described by the functions

they perform, specifically by the way they reconcile basic values with technological change and by the way they provide for educating the participants in the legislative system.

A. Basic Functions

The complexity of information processing is reduced if the data subject understands the information environment. All data protection laws, therefore, include provisions that, though by different means, require the user to disclose either general or specific information to the data subject, *e.g.*, where personal information is being processed, where the user obtained the information, and where the user will send the information. The means by which a data subject can obtain this information differ according to the approach of the particular law; the information can be found in general directories, the data subject can demand the information directly from the user, or the law can require the user to provide the information after specific transactions or on a periodic basis.

While openness is the prerequisite, the actual reconciliation of informational conflicts has to be achieved by balancing mechanisms. Since the concept of technology laws does not contemplate deciding all possible conflicts in advance, each specific law has to provide a mechanism by which different interests can be sufficiently discussed, balanced, and then decided. Data protection laws provide for two basic balancing mechanisms: the implied and the explicit analysis of conflicting informational interests. Implied analysis occurs when the specific data protection regulation allowing or prohibiting information handling already contains a process of analysis and balance. Explicit analysis occurs when a particular handling of data is not regulated by a law and its implied mechanism for balancing conflicting interests.

Personal data generally may be processed if the data subject has given his/her express consent. The law simply assumes that the data subject has given his/her informed consent, *i.e.*, the person concerned has weighed the competing interests for him/herself and has come to the conclusion that processing should be favored.[13] Since it would be too complicated to ask for or to provide such consent any time personal data is going to be processed, another implication generally is included in the consent mechanism. In other words, no express consent is necessary if the data subject has reason to assume that personal data is going to be processed in a par-

13. Further problems, such as whether the data subject had "real" freedom to refuse consent, and such as what constitutes "informed" consent, have been discussed widely in data protection literature and will not be discussed here.

ticular social situation, *e.g.*, in a contractual relationship. It is assumed in such a case that consent to the particular social interaction is tantamount to consent to the handling of information.

Apart from these personal or social situation orientated mechanisms, one finds implicit interest analysis mechanisms in special laws. These mechanisms are usually in the form of explicit handling regulations in the data protection law itself, usually for particular sectors (*e.g.*, mail address companies in Denmark), in special data protection laws (*e.g.*, The Credit Reporting Act in Sweden), or in "unspecific information laws" (laws that cover information handling inter alia, *e.g.*, tax laws that contain regulations for information transfers from the private to the public sector). The implicit interest analysis principle applies here because it is assumed that the legislators have specifically weighed the prospective interests of the persons involved in a specific information relationship against the interests of those who are to give or receive that data.[14] The decision reached by the legislators is legitimate, therefore, under the principles of democracy.

In many cases, however, there is data handling without the consent of the data subject and without a legal mechanism for balancing the conflicting interests. Such transactions occur frequently and range from trivial (*e.g.*, a company collects addresses for marketing by mail) to serious (*e.g.*, two or more insurance companies combine the file of an individual suspected of making dubious claims). There must be explicit analysis in these cases. Since neither the person concerned (consent mechanism) nor the legislator (specific law mechanism) undertakes the balancing in a specific information relationship, the data user or a special body must perform the task. Sometimes, but not always, data protection laws provide guidelines for striking the balance, but because of the generality of the legal terms, it is debatable whether the user has to carry the risk (if it becomes a court case) or an appointed body has responsibility for making the decision.

Finally, it is obvious that the mechanisms of balancing interests

14. The "specific law solution" is the cause of many misunderstandings regarding the European approach to data protection. Although the data protection laws of Western Europe take an omnibus approach (in contrast to the sectoral approach of the United States), they do not override other regulations regarding the handling of personal information. In Germany, for example, the data protection law explicitly states that it is subordinate to specific regulations that are contained in other statutes. Many regulations regarding employer/employee information relationships consequently are found in labor or similar statutes or in cases interpreting those statutes. The implied or explicit subordination, however, poses specific problems of interpretation that cannot be dealt with here.

define the quantity and kind of data as well as the interests of those participating in the communication process. Since interest analysis demands the discussion of the purpose of particular data handling in a particular context, any decision in favor of processing is limited by that particular purpose: there must be new and specific analysis for *any* other purpose. One finds in all these laws, therefore, rules that demand a rationalization and a minimization of data handling according to the particular purpose the information transfer is designed to serve.

B. Basic Approaches

Explicit interest analysis and balancing must be implemented. Among the options available for implementing these principles, alternatives emerge. The law can require (1) the user to register or to obtain a license (ensuring openness); or (2) the user to police himself (substantive approach).

The substantive approach leaves it up to the user to see that the principles of data processing are duly applied. In such a system, openness usually can be achieved only by allowing a right of access or by using a rule that requires notice to the persons concerned because there is no administrative process for collecting general information. The other approach demands that a special procedure be followed before a personal file may be established. Such a procedure may vary from strict licensing to simple registration. In order to obtain a license, details of the system would have to be provided concerning the kind of data, the mechanisms for ensuring correctness and for providing access to the person concerned, the responsible personnel, the regular recipients, and the purpose of the data collection or communication. An appointed authority would then check whether the principles and mechanisms described were being followed (the authority also usually rules on the acceptability of the system). The license generally would be issued upon payment of a fee, limited to a prescribed time, and revoked for any modification of the system. A registration system would require a registration authority with the same powers as listed above, but the system could begin operating at the moment of registration or as soon as the user receives a receipt. The authority usually has no discretion to refuse registration, but in some cases one may be asked, however, to explain the system further.

Describing data protection laws in an "ideal type" manner was necessary to understanding the context in which data protection agencies operate. In practice, however, all data protection systems with which this Article is concerned contain a mixture of balancing

mechanisms and approaches. Implied balancing in the form of consent is very common in private sector regulations and the "specific law mechanism" is used mostly in the public sector. Explicit analysis and balancing usually is used for specific information systems or user groups that process sensitive information. The Swedish system, usually associated with the licensing approach, in fact accepts registration for the more common personal files provided the general regulations set up by the data protection authority are being followed. The German system, regarded to be the prototype of a substantive approach, nevertheless asks for the registration of specific user groups in the private sector.

III. THE ROLE OF DATA PROTECTION INSTITUTIONS

The functions usually associated with data protection agencies in Western Europe include providing openness, undertaking interest analyses, making explicit balancing decisions, and performing registration and licensing procedures. Before further analyzing how these institutions perform the functions assigned to them by the various laws, a short survey on existing institutions shall be presented.[15]

A. Data Protection Agencies in Western Europe—A Brief Survey

Austria

The Austrian data protection law created the Data Protection Commission and the Data Protection Council. The Council consists of representatives from political parties in the Federal Parliament, from the Federal State, the Laender, and the local communities, from private enterprise interest groups, and from employees' organizations. The Council oversees the general development of data protection and has the right to investigate data processing in the public sector in order to judge its lawfulness. The Council also serves as a forum for general discussion and submits a report to parliament once every two years.

The Data Protection Commission consists of four members that are nominated by the government and appointed by the President. It has the right to be heard regarding regulation of personal data processing in the public sector. It administers the register for both

15. Only a short survey can be given here. A more detailed survey, if only of the state of the art in Sweden and EEC countries as of 1979, is available. *See* 2 H. Burkert, The Organization and Practice of Data Protection Agencies, EEC Joint Study on Data Security and Confidentiality (1980).

the public and the private sector, but the National Statistical Authority, which has to be consulted if registration is refused, keeps the register. The Commission handles complaints against public sector data processors and assists in handling complaints against private data file keepers. The complainant, however, must follow regular court procedures.[16]

Denmark

Denmark has separate laws for the private and the public sector, but the control authority, the Data Surveillance Authority, has jurisdiction over both sectors. The agency consists of a Council and a Secretariat. The Council has seven members who are appointed by the Minister of Justice, and the Secretariat was slated to consist of twenty-five members in 1980. The Council makes decisions of a general nature and supervises the work of the Secretariat, which executes day to day business.

In the public sector, the Data Surveillance Authority supervises all data banks to which the Public Registers' Act refers. It gives its opinion regarding changes in the law, projects installing data banks, and file matching between public data banks. It also has the right to investigate complaints. In addition, the Authority can ask for specific information about public data banks that are set up by directives from a ministry. An annual report must be given to the Danish Chamber of Deputies.

In the private sector, the Authority ensures that the regulations of the Private Registers' Act are kept. Specifically, the Authority gives its opinion on intended modifications of the law, it investigates complaints, and it keeps a register on credit information and computer service bureaus. The decisions rendered by the Authority can be challenged in competent courts.

France

The Data Protection Commission (Commission Nationale de l'Informatique et des Libertes) consists of seventeen members, each appointed by various state organs.[17] The Commission is supported by an administrative department that employed about twenty people in 1980. The Commission draws up simplified regulations for the most common forms of personal data processing in both the public

16. Further details are available. *See* K. BEDNAR & M. WEISSENBOECK, DATENSCHUTZHANDBUCH (1979).

17. The Commission's own report supplies further details. *See* RAPPORT DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES, BILAN ET PERSPECTIVES, LA DOCUMENTATION FRANCAISE (1980).

and the private sector. In the public sector, it gives its opinion on new laws or regulations establishing personal files.[18] In the private sector, the Commission receives a notification of intent to set up personal files that has to be acknowledged. In cases involving a simplified procedure, the Commission receives only a simple declaration.

Federal Republic of Germany

The data protection system of Germany is somewhat complicated because of its federal nature. There are three different types of data protection agencies. The federal level public sector is controlled by Federal Data Protection Commissioner, who applies the federal data protection law. The various Data Protection Supervisory Agencies, which are part of the Laender administration control the private sector by applying the same federal data protection law. The Laender Data Protection Agencies (sometimes commissioners or a board) control the public sector on the Laender level according to the specific Land's data protection law.[19] The Federal Data Protection Commissioner's office, which is of main interest here, had about thirty employees in 1979/80.

The control authority (the Federal Data Protection Commissioner) keeps a register on personal files in the public sector on the federal level and deals with complaints from the public. It ensures cooperation between the various data protection authorities and gives advice in data protection matters. The control authority carries out inspection and can admonish public authorities, through their supervising authorities, in order to ensure that data protection measures are enforced. Finally, the control authority gives an annual report to the German Parliament.

Luxembourg

The tasks of data protection agencies are shared between the competent ministry (*e.g.*, the Ministry of Justice), which acts as a data protection agency in the proper sense, and the "Commission consultative," which, as the name indicates, has a consulting function. The Luxembourg data protection law establishes a licensing system for the private sector. The licenses are administered by the

18. This is more than the usual "opinion" since a negative decision can be overruled only a decree from the Conseil de l'Etat.

19. In addition, there is a system of internal control in the private sector. Firms performing a specified level of personal data processing must appoint data protection commissaries. This is mainly a counterpart to the substantive nature of the data protection law and the relatively limited power of the supervisory agencies.

competent ministry and entered into the National Data Bank Register, which also contains information on the personal file systems of the public sector. These systems can be established only by law or decree, and only after the systems have been assessed by the Consultative Commission. Investigations and interventions in both the public and the private sector can only be made, however, by the competent ministry. Infringements have to be reported to the criminal prosecution authorities.

The five members of the Consultative Commission are appointed by the Grand Duke, represent the public and private sector, and include computer scientists and legal experts. The Commission has the power to initiate research and is required to supply general information about data protection and information technology questions, to advise the government, and to give an annual report.

Norway[20]

The data protection agency for Norway, the Data Inspectorate, is a seven person board that, in April, 1980, included four executive officers, two office personnel, and the director. The primary public sector function of the Inspectorate is to give opinions on drafts of new statutes that relate to data protection issues. In the private sector, the Inspectorate administers concessions for all electronically aided personal data registers and such non-electronic personal data registers that store sensitive information (*e.g.*, medical information). Registers in the public sector that are not covered by specific statutes and that are not exempted explicitly fall under the same jurisdiction of the Data Inspectorate as private registers. The Inspectorate also may establish more precise rules, or may modify or make exemptions from specific rules that concern all other personal registers or specific types of registers. Additionally, the Data Inspectorate keeps a register on all these data files and has a broad, though not absolute right to inspect them. Finally, any decision made by the Inspectorate may be appealed through the Ministry of Justice.

Generally, the Inspectorate must keep informed of developments regarding data protection issues and, in this respect, it must give advice and guidance to parties who are planning to establish registers. The Inspectorate also must ensure that the data protec-

20. Detailed descriptions of the Norwegian system abound. *See* Føyen, *Implementation of the Norwegian Personal Data Registers Act*, 2 INFORMATION PRIVACY 190 (1980); Selmer, *Norwegian Privacy Legislation*, 1 INFORMATION PRIVACY 178 (1979); *Focus on Norway and Sweden*, 1 TRANSNAT'L DATA REP. (1978).

tion regulations are observed, and that errors and deficiencies are rectified.

Sweden

Sweden's data protection authority is the Data Inspection Board. The actual board supervises the activities of an administrative department (comprised of about thirty persons at the beginning of 1980). The board includes the director, representatives from the political parties and unions, and experts in public administration, computer science, and medicine.

The Data Inspection Board keeps a register on personal files in both the public and the private sector. The Board administers the private sector licensing system, which may require either a standardized or a specialized procedure, depending on whether the file for which a license is sought comports with the more common forms of personal files or whether it is considered unique. The same regulations apply to files in the public sector; if, however, the public sector was set up by law or directive, the Board must be *consulted* regarding file specifications. Finally, the Data Inspection Board has the right to investigate complaints and make inspections on its own account. Appeals from decisions of the Board are to be decided by the Ministry of Justice.

B. General Functions Within the Concept of "Technology Law"

The general features of technology law, as described in part I, include the need to make the legislative system learn. This need can be satisfied by establishing a sensor that reacts to difficulties in implementing data protection regulations. A specific sensor is needed if data protection regulations are embodied in a "steering" system. At the present stage of regulation, however, sensors are needed more for knowledge than for actual steering, so data protection agencies collect information, monitor general developments, and report their findings to the legislators or the government. Registration and licensing procedures provide further special information.

Changes deemed to be necessary by the sensor must be communicated to the appropriate authorities and also to the users, the subjects, and the public. Data protection agencies, in which knowledge and expertise about data protection is concentrated, perform this task on several levels and by several means. They educate the general public by participating in forums, by producing brochures, and by making media appearances. They educate users by issuing

informational booklets or manuals,[21] or by supplying specific information when discussing a particular licensing application. They give data subjects a general education or they give advice in specific cases. Finally, they advise governments and legislators and thus participate in making information policy.

C. Specific Functions Within the Mechanism of Data Protection Laws

Apart from these general functions, agencies also act within the specific demands of privacy law, providing openness, analyzing and balancing interests and, not yet mentioned in this context, exercising control. Openness usually is provided by establishing records on personal files systems and by making them accessible to the general public. Data protection agencies balance interests in the public sector by giving their opinion on the law or directive that implements the personal information system. They are involved, therefore, in the "implicit interest analysis" while legislation is being drafted. In the private sector, the agencies perform "explicit interest analysis" whenever they modify or refuse applications.

Although the control function has not been referred to in the general context of technology law nor in the specific context of privacy law, its existence is self-evident. This function, at least in its isolated form, has drawn much attention, but it tends to be of less importance in everyday practice because the main function of a "type two" technological law is to learn. Strict control may close informal information channels, which in turn may lead to wrong or "overemphasized" decisions. Such decisions may endanger co-operation and jeopardize acceptance by the users. Co-operation is necessary for agencies to operate with efficiency.[22] Consequently, representatives from data protection agencies emphasize their advisory functions: when conflicts arise, they seem to prefer bargaining to prohibitive measures.

Ironically, providing openness and balancing interests necessitates some control. The regulatory agency can no longer be left

21. The Federal Data Protection Commissioner in Germany, for example, has circulated more than 60,000 copies of his information brochures. It is one of the "best-selling" (it is free) governmental information booklets. The Swedish Inspectorate has gone as far as printing data protection information on milk packages.

22. Problems usually are sorted out in direct discussions with the authorities. This may be due to the fact that both parties depend on each other during the implementation period. "Friendly" administration is not altogether unproblematic since it may weaken the authorities' ability to achieve general acceptance. A research project of the Norwegian Research Center for Computers and Law currently is looking into this problem.

without control because the usual authorities may lack sufficient flexibility or the specialized knowledge needed to administer control. Not surprisingly, data protection agencies find themselves in a difficult position: they must balance a flexible and cooperative policy with control. Neglecting control would endanger the credibility of data protection laws and would make acceptance by data subjects impossible. One of the main arguments for an institutional approach is that such a balance can best be kept by a separate institution with special expertise and capability.

How can a data protection agency achieve control technically? As pointed out in the brief survey, data protection agencies have a general right to inspect, either directly or by applying to the proper juridical authorities. Considering their limited resources, these agencies have been relatively effective in their inspection procedures thus far. One reason for this success seems to be their concentration on organizational deficiencies during their inspections. Such faults, though relatively easy to detect, are of vital importance for the decision output of such organizations. Preventive control, *i.e.*, the agencies' influence on subsequent licensing or registration decisions, also helps to reduce the need for inspections. The public's right of access and public's ability to call in the agencies if there is reason for suspicion provide additional control and further reduce the need for inspections.

IV. AN ATTEMPT TO EVALUATE THE INSTITUTIONAL APPROACH

Legislators who wish to learn from the experiences of other countries, and the history of data protection in Western Europe is a good example of legislators helping each other, would like to know if there are viable alternatives to data protection agencies. Though some general problems of data protection have led to similar general solution structures, such a question is connected too closely to the political and legal traditions of any one country to have a clear answer. Any evaluation of this question, therefore, can be only of a general nature. Some functionally equivalent options that, to a certain extent, have been discussed in the reports preceeding data protection legislation, will be discussed briefly. There are, however, some consequences that deserve broader attention since they may lead to a long term change for the data protection agencies or for the entire system of information control. These consequences might flow from the relationship between data protection agencies and the traditional institutions of political power.

A. Functionally Equivalent Options and Reasons for the Institutional Choice

Considering the general functions of technology laws and the specific functions of data protection laws, the choice not to institutionalize data protection can mean having these functions performed by existing institutions, or it can mean relying on non-institutional mechanisms. The usual method of implementing a law is to leave it to the juridical power to oversee the law. None of the existing Western European laws excludes the possibility of seeking the help of the courts or some other body to override the decision of the data protection agencies. Only the Austrian law states explicitly that, in the private sector, the data subject him/herself has to seek the help of the courts; the Data Protection Commission can only give assistance. The Western European Community apparently does not regard courts as functionally equivalent options, especially in light of their reliance on additional safeguards.

Not installing special agencies and relying exclusively on the courts also would imply a purely substantive approach. The courts would be left to act as the only sensors and advisers unless the traditional information collecting agencies (*e.g.*, statistical offices) or advisory institutions (*e.g.*, chambers of commerce, consumer aid, and user organizations) agree to split these tasks among them. Since this is often very costly and time consuming, another option has received wide attention: the self-regulating mechanism.[23] In such an approach, users or groups of users set up their own institutions or hand over the desired tasks to existing ones already under their administration. These institutions would regulate the proper handling of personal information and would give any assistance needed. These solutions have received much interest, especially in countries with experience in strong self-regulating professional standards, because such methods could foster development of ethical standards from within rather than from enforcement from without.

The prevailing regulatory philosophy of Western European legislators, however, is evident in the following statement: "[The government] opted for the strict, bureaucratic solution, well aware that it would cost more and might hamper administrative activities . . . . 'Because of anxiety that many people probably feel *vis-a-vis* the modern personal data registers, . . . it is important to keep the development under control as much as possible.' "[24] Though the con-

23. *See* Kling, *Models for the Social Accountability of Computing*, Telecom. Pol'y, Sept. 1980, at 166.

24. *See* Selmer, *supra* note 20, at 180.

trol function seems to be less important in practice, it was believed that a separate and independent body, rather than the courts, would be better suited for the delicate task of balancing interests in order to make a new technology acceptable. As an added advantage, the agencies would act to focus the issues for the courts if the courts were subsequently needed.

The decision in favor of the institutional approach, therefore, has to be seen in close connection with the social mood that helped create the new technology law. The social mood is important to the analysis simply because the legislative action was deemed necessary in the first place only because the problem area was regarded as sensitive or at least as having the potential for important social conflict. Since the effect of these laws had to be constantly watched, and since the legislature itself could not keep in touch with these developments, a functional need arose for an appropriate institution that, at the same time, would help in reassuring the public that "somewhere someone" was taking care of the problem area.

B. A Problem Area of the Institutional Approach: Data Protection Institutions and Traditional Institutions of Political Power

The discussion of the relationship between courts and data protection agencies points directly to a fundamental problem area: the relationship between data protection agencies and traditional institutions of political power.[25] For practical reasons, the traditional model of the division of power between the executive, the legislature, and the judiciary shall be maintained as a reference model, though it is no longer valid in this clear abstract form. Keeping in mind the weaknesses of the reference model, three general assumptions may be made:

- Data protection agencies will concentrate and amplify political power to a great extent;
- This concentration and amplification will lead to conflicts with the executive, the legislative and the judicial powers;
- In the course of these conflicts, the institutional approach that has been implemented so far will need some fundamental reworking.

Concentration and amplification can be explained in the following manner. Information policy is becoming more and more important as its security and economic implications are being realized.

25. *See* Burkert, *Datenschutzbehoerden als Kontrollinstanzen der Information?* in Informations-systeme fuer die 80iger Jahre 354 (1980).

Data protection is a part of, though not always a well integrated part, of information policy. Integration is difficult partly because the area to be regulated by the agencies, though defined to some extent by data protection laws, can never be completely defined since the concept of "technology law" contemplates these agencies needing and using maneuvering space. This is the only way that the agencies can keep track of technological change, can remain flexible when balancing interests, and can adapt to the specific character of data protection.

In the course of performing their mandates, data protection agencies combine acts of policy planning with acts of policy making, individual decision making, and control. They play a part in policy planning because they have accumulated expertise to an extent that no policy maker can. They make policy whenever they give advice, or whenever they prescribe or recommend types of personal systems. They make specific decisions whenever they refuse or modify licenses or registrations. In other words, various forms of political power are concentrated in these agencies.

Power is not only concentrated but amplified by the ability of the agencies to adapt to the information environment. The agencies are superior to the more traditional forms of public administration in the way that they use their powers. Their personnel, who can be chosen more freely by the leading officials of these institutions, usually combine skills from the legal and information sciences, a combination that seems to be well suited to solving problems of informational technology. Representatives of these agencies are able to talk the "information language," to present and solve problems of information power, and to accumulate even more practical experience. They use informational technology themselves in managing their various tasks. They can be judged, therefore, at least for the time being, to be better prepared to handle problems of information power in a societal context than other parts of the public sector.

The role of data protection agencies in the public sector has not be analyzed sufficiently yet. Current international surveys concentrate on the role of data protection agencies in the private sector in order to attract the interest of international users. Most analysts would agree, however, that there are two general ways that these agencies exercise influence in the public sector. They participate in the development of governmental or public administration personal files and/or they control the existing systems. This usually puts the agencies in a difficult position: in theory, they are part of the executive branch, yet they are supposed to counterbalance concepts of efficiency with the interests of the persons concerned. In addition,

they must check and possibly challenge administrative procedures. As such, they perform internal control for the executive branch. Other institutions that perform similar functions in public administration systems (*e.g.*, budget control) are in a similar position. Like these institutions, data protection agencies must take precautions to try to avoid being taken hostage by the administration. Although the agencies are sometimes technically established within the administrative structure of a ministry, their head officials usually have judicial status, which makes it impossible to remove them from office for any reason other than those that would make a judge unfit for office. By reporting to the legislature, the agencies can strengthen their position generally and ensure that the general public is aware of important conflicts. Other administrative units cannot overrule their decisions.

Reports of these agencies suggest that conflicts with the administration, and thus with executive power, play an important role in everyday operations of data protection agencies. These conflicts seem to play a more important role than the conflicts created by other internal control mechanisms, mostly because publicity is assured by the reporting mechanism and also because the area of information processing receives intense attention from the general public. The fact that issues of state security are often at stake in such conflicts adds to the attention. These reasons, however, also may lead the data protection authorities to seek mechanisms of conflict regulation that do not attract too much publicity, to be cooperative in order to realize their concepts to some extent, and to calm down controversies. At the same time, however, they are reminded continually that their credibility is at stake since they can only achieve acceptance if they can be trusted to offer sufficient resistance. In sum, conflicts with the executive play a vital role in the performance of data protection agencies and much attention should be given to the possible solutions of such conflicts.

Conflicts between data protection agencies and the judicial power have received little attention so far. It generally is assumed that no such conflicts occur since all decisions of the data protection agencies can be challenged in court, in court-like institutions, or at the highest administrative level. In fact, only the Austrian law has given the matter some attention by clearly defining the advisory role the Data Protection Commission plays in the private sector. Other data protection laws do not contain such explicit emphasis, which seems to indicate that no specific conflict has been noted. Conflict, however, may not be totally avoided. Data protection agencies presently may exercise impact on court decisions, even if only as advi-

sors, as long as judicial expertise has room for growth and external advice is difficult to obtain.

The data protection agencies' selective function in taking legal action is of equal importance. This does not necessarily influence the role of judicial power since specific bodies normally are assigned a selective role, but it may have an impact on the data protection agencies themselves. The agencies may feel reluctant, at least for the present time, to bring specific cases into court because they want to avoid decisions by "unprepared" courts that may have a restrictive influence on their practice. As a result, data protection agencies may prefer out of court settlements as long as they feel a lack of experience and as long as they wish to probe their own field of operation. This function of "mobilizing law" will need further attention.

The main source of possible conflict, however, lies in the relationship between data protection agencies and the legislature. As previously explained, data protection agencies have a broad margin for decision. This implies a certain power of interpretation that may lead to a deviation from the intentions of the legislature. Even though they received their legitimation from the legislature, data protection agencies can become relatively independent because the necessities of technology law demand wide agency discretion. Courts and administrative agencies always exercise discretion when they interpret law, but the margin in this area is relatively broad, the power of the agencies is relatively strong, and the area in which these agencies operate is extremely important because of its infrastructural character.

Many legislatures may have anticipated possible conflict since some of the Western European models include a strong connection between data protection agencies and the legislature. This "connection" may consist of organizational orientation toward the respective parliamentary bodies, either by making the agencies' responsible to parliament, by making the agencies report to parliament regularly, or by appointing members of the parliamentary body to the agency boards. These assumptions are directed toward the future and it remains to be seen how the participants of possible power conflicts will react to these developments. The problems, however, have been realized by countries that are contemplating legislation.[26]

26. The legislative character of codes of practice has been a controversial issue. *See, e.g.*, LINDOP REPORT, *supra* note 3. In Germany, the expertise function in the area of social security research recently was given to the social security administration itself instead of to the Federal Data Protection Commissioner. The European Parliament has stressed the importance of including the parliament in any institutional model for data protection in the EEC. *See* PROTECTION REPORT, *supra* note 4.

CONCLUSION

The "European approach" to data protection, and the implementation of data protection agencies in particular, must be viewed in close connection with the prevailing public mood toward informational and communications technology. Although not fundamentally hostile toward technological change, the public has taken a more cautious attitude. This attitude most likely is connected with past abuses of information and communication power and with present consciousness of the cultural implications on a multilingual continent. Such an attitude makes legislators sensitive to value problems involved in technological change, particularly in informational and communications technology. Their legislation, therefore, tends to use a cautious approach, trying to learn while trying to reconcile structural changes with prevailing traditional values in order to avoid abrupt changes. In the still highly specialized area of informational and communications technology, legislators felt it necessary to hand over these learning and reconciling functions to specialize institutions rather than to leave them with traditional ones. This may become, in the long run, the cause of future conflicts; at present, however, these institutions seem to perform reasonably well. One can envision, nevertheless, a time when these specialized institutions of information control may become obsolete, when general awareness of the value problems of information and communication technology will have been achieved, when public and private users alike will have made their systems sufficiently open, and when the individual or any group of individuals will feel sufficiently confident and equipped to participate in communication no matter how complex the technology may be.

These are signs of the rising sensitivity to the political power of data protection agencies.