Information technology and civil liberties

STEINMULLER, Wilhelm; Poullet, Yves

Publication date:
1989

Document Version
Publisher's PDF, also known as Version of record

INFORMATION TECHNOLOGY AND CIVIL LIBERTIES

James MICHAEL, Yves POULLET and Wilhelm STEINMÜLLER. ~~(eds.)~~

~~1988~~

"Civil liberties", in the traditional sense, are those human activities which should be as free as possible from state control. The expression "civil rights" has two distinct meanings: in civil law countries with a Roman law tradition, the term "droit civil" means ordinary rights in private law, such as the right to enforce a contract in common law countries. The term is more closely related to "civil liberties" in meaning legally enforceable rights, usually against the state. This distinction, very roughly derived from the legal philosophy of Hohfeld, has particular application to information.

"Civil liberties" and "civil rights" are both about power relationships, largely concerned with the relationship between the individual and the state. In the famous phrase of Bacon "information [or, rather, knowledge] is power", although it is of course not the only kind of power. Information technology, at the very least, greatly increases the potential uses of that power (it is not coincidental that people in information technology routinely speak of "computing power"). Law is not the only influence on the power relationship between individuals and the state (and other institutions) concerning power; but it can be an important one.

Two particular legal developments are relevant to information technology and civil liberties/rights, usually described as data protection and "open government" ("transparence administrative"). Data protection is a specific application of some principles of privacy (itself only recognized as a legal concept since the end of the 19th century) to information technology and has as its purpose the protection of individual autonomy over personal data. "Open government" laws usually take the form of public rights of access to government records, with the purpose (one purpose, at least) of making government more accountable to the governed. Together, they are attempts at redressing the balance of information power. They are attempts, however imperfect (and some are very far from perfect) to avoid Ellul's prediction that technology enables the state to absorb the citizen's life completely. They do this by protecting the citizen's information autonomy and making government more transparent. It is perhaps significant that the principles of open government and data protection are not specific to information technology (although some data protection statutes are).

The earliest legal expression of these concepts was probably in the Swedish law of 1766, called the Freedom of the Press Act (although not at all limited to the press) with emphasis on open government ("öffentlicheitsprinzip"). It was not until the middle of the 20th century, however, that legislation on both subjects began to spread. "Data protection" laws have been more specifically related to information technology, and have been more co-ordinated in international law through

the Council of Europe's Convention on Data Protection and in non-legal codes such as the OECD's Guidelines. There are now approximately seventeen countries with data protection or open government laws (many, like France, with both) and the number is growing.

This paper does not attempt to survey those developments. Nor does it attempt a thorough account of the law in any particular country, which would be much longer and probably limited in interest to lawyers. Instead the authors describe particular aspects of information technologies and civil liberties in the legal traditions most familiar to them. James Michael's account of developments in international law is followed by a summary of the common law approach to privacy and open government. Yves Poullet describes French legislation on data protection and open government together with related developments such as Minitel. Wilhelm Steinmüller analyses the civil liberties issues presented by information technology in the Federal Republic of Germany and concludes the paper with a caution on the limits of legal regulation. The emphasis throughout is on the legal solutions attempted to the problems of civil liberties presented by converging information technology; the issues are not new, but the scale and impact presented by technology is. These are, in effect, snapshots of civil liberties in the landscape of an information society.

1. International and European Law

Although the right to privacy is proclaimed in Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, Article 5 of the American Declaration of Rights and Duties of Man, and Article 11 of the American Convention on Human Rights, the most productive expression has been in Article 8 of the European Convention on Human Rights. Space does not permit an account of the case-law under it, but in Dudgeon v. the United Kingdom[1] the Court held that the Northern Ireland statute making male homosexuality a crime violated the Convention. In October 1988, the Court also ruled, in Noris, that a similar law in the Republic of Ireland also violated the Convention.

The development of the international law of data protection began with general rights to privacy in international instruments, and continued with particular emphasis on the privacy problems presented by new information technology during the 1970s. Much of the impetus for what emerged as the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was commercial. It was thought that conflicting national laws on data protection might be used as non-tariff trade barriers to hinder the new international markets in information.

The institutions of the European Community were particularly concerned about the possibility that such non-tariff trade barriers might be used to circumvent the Treaty of Rome's rules about free movement of

[1] (1981) Series A, Vol. 45.

goods and services within the Community. It is at least possible that the urgency of this concern was the reason why the EC deferred to the larger and older Council of Europe in establishing international rules. The reason for the shift to the Council of Europe (which is now being repeated with satellite broadcasting rules) is mostly to draft a set of rules as quickly as possible. Community legislation usually takes the form of a directive which is binding on all Community members and requires implementing domestic legislation. Precisely because it will bind every member state, the process by which a final directive is arrived at can be protracted. In contrast, the "legislation" of the Council of Europe is in the form of Conventions which members may sign and ratify or not. The process of arriving at a set of rules can thus be much faster, and not subject to any country's veto. When the Convention is open for signature and ratification membership in the "club" is thus voluntary, although there often are political and economic pressures to join. Thus, regional international law on data protection is now relatively settled in the Council of Europe's Convention (which may be adhered to by non-European countries), and the principles are also reflected in the OECD Guidelines. The next step is likely to be detailed implementation and interpretation. The general right to privacy is also being developed at national and international levels. As the U.S., Irish, Canadian and European Convention cases will illustrate, this presents interesting opportunities for cross-fertilization between different legal systems.

2. Common Law Privacy

There have been many different paths of development in different legal traditions that led to the human right to privacy in international laws. Some traditions emphasize the right of personal honour, others the right of physical privacy in the home, others the freedom to develop one's personality, and others the protection of family life; some have developed by statutes and others by judicial creativity. The right to privacy in Anglo-American law developed through both case law made by judges and legislative statutes before it emerged as a human right in international law.

Although the expression of a legal right to privacy seems not to have been used until the middle of the 19th Century, there were earlier developments in common law countries which would now be recognized generally as privacy protection measures. In the literature on privacy in common law countries, three particular developments stand out. The first was an English case in 1849, and the third a decision of the U.S. Supreme Court in 1965 (see below).

The English case was that of Prince Albert v. Strange[2]. Queen Victoria and the Prince Consort had executed some etchings which came into the hands of a man named Strange, who proposed to exhibit them and to publish a catalogue describing them. The catalogue is particularly important because it would have communicated information about the

2 41 English Reports 1171.

etchings, rather than the original etchings themselves (which would have been protected under the law of theft) or copies of them (which probably then, and certainly now, would be protected by the law of copyright). Prince Albert's argument for an order to stop the exhibition and publication of the catalogue was based on a doctrine known as the law of confidence.

Prince Albert got his injunction from the Vice-Chancellor, who referred in passing to the "right ... of privacy". But in the years since that decision the common law has yet to involve a general right to privacy in England (the law in Scotland is slightly closer); such evolution was left to the courts and legislatures in North America, where the wedding of the daughter of a Boston attorney named Samuel Warren was the rough equivalent to the royal couple's etching.

Mr. Warren did not like the publicity given to the wedding in the local newspaper. Perhaps unusually for an American lawyer, instead of taking legal action against the newspaper he wrote an article about the subject with his partner Louis Brandeis (later to become a justice of the U.S. Supreme Court). The article, *The Right to privacy*, appeared in the Harvard Law Review in 1890. In it, Warren and Brandeis argued that several common law doctrines, such as the law of trespass, defamation, and breach of confidence, amounted to a single right to privacy when taken together. This was followed rapidly by state laws protecting various aspects of the right to privacy, probably the first of which was the New York state law protecting against the commercial exploitation of one's image. The courts rapidly began to develop the tort of invasion of privacy, and in 1960 these were classified by dean Prosser of the University of California as the torts of intrusion, disclosure of embarrassing private facts, presenting an individual in a false light, and appropriation of a name or likeness [3].

In 1965, the U.S. Supreme Court went one step further. Until Griswold v. Connecticut[4] the right to privacy had been, developed as a common law or statutory right, but not one of constitutional status. In that case the Supreme Court used judicial reasoning very similar to that of Warren and Brandeis: putting together specific provisions of the Bill of Rights such as the right against unreasonable searches and seizure and the rights to freedom of religious belief and speech, the Court found that in their "penumbra" was a constitutional right to privacy. One aspect of that was the right to sexual privacy, and a state law regulating the sale of contraceptives was held invalid as it violated that right.

This was followed by Stanly v. Georgia[5], in which a state law prohibiting the viewing of pornographic films at home was ruled unconstitutional. In 1973, the Supreme Court took another step, and ruled in Roe v. Wade[6] that a woman's right to privacy was violated by statutes limiting her ability to obtain an abortion, at least during the first trimester of pregnancy.

---

3 48 California Law Review 383

4 381 U.S. 479

5 394 U.S. 557 (1979)

6 410 U.S. 113

In Ireland the right to family privacy is established by Article 41.1.1 of the Constitution, and in McGee v. Attorney-General[7] it was held to be violated by a law forbidding the importation of contraceptives. Anticipating that the Irish Supreme Court might follow the path of the U.S. Supreme Court in moving from contraception to abortion, a successful campaining was mounted to amend the constitution to ban abortion.

In Canada, Section 7 of the Charter of Rights of 1982 establishes the "liberty and security of the person". In a decision which rarely uses the word "privacy", but which nonetheless is very similar to Roe v. Wade, the Supreme Court of Canada has recently held the Canadian law regulating abortion to be unconstitutional. Meanwhile, the U.S. Supreme Court has withdrawn somewhat, holding in Bowers v. Hardwick[8] that a state law making homosexual (and perhaps some heterosexual) acts criminal did not violate the right to privacy.

The common law countries have not followed civil law countries in adopting technology-specific data protection laws. Instead they have legislated to establish rights of privacy and general rights of access regarding government records. This is broader than many data protection statutes, in its application to both manual and automated records, but it is more narrow in applying largely to the public sector. The U.S.A. has both the Freedom of Information and Privacy Acts, while Canada has a combined Access to Information and Privacy Act, but has not yet legislated regarding privacy at the federal level. New Zealand has a technology-specific law regulating the police national computer and relatively weak access to government records law. Space does not permit detailed discussion of these laws, but they have several characteristics in common. They all establish a relatively impartial arbiter for disputes over information between citizens and government, and many establish rights of correction and compensation for the misuse of information about people. There is much to be done, and always the danger that symbolically reassuring legislation can do more harm than good: but there has been a beginning.

3. Roman Law Tradition: The French Case

Under this title, only the French case will be considered, one reason being that the laws concerning "Information Technology and Civil Liberties" are more developed in this country than in other Roman Law countries like Belgium, Italy, Spain or Portugal. A more important reason is the feeling that the French approach is quite unique compared with the German or English one. The French regulatory framework is focused very much on the citizens' right to obtain information from the public sector (3.1.) with a view to protecting the same citizens against misuses of information by public or private sectors (3.2.).

---

7 1974 Ir. R. 284

8 92 L. Ed. 140 (1986)

A second original feature of the French case is to create a legal framework anticipating the convergence of the various media, stimulated by the new technologies of telecommunication, and to submit the different forms of communications, including audiovisual programs, to global solutions: this is legal creation of a new "Communication Order" ("Ordre de la Communication") (3.3.).

3.1. Computer and Liberties: Debate and Trends

In January 1978, the French Parliament enacted legislation entitled "Computer and Liberties". The purpose of this regulation was both to provide adequate protection for privacy against misuse on the part of private entreprises or public administrations and to envisage a way to regulate the impacts of the computerization of society on the various civil and public liberties: "Information technology must serve the citizen ... it should not endanger either human identity, human rights, privacy, or individual or public liberties" ("L'informatique doit être au service du citoyen ... Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques").

The French commission on Computer and Liberties (CNIL), which was created by the Act, has made a number of suggestions in respect of new services created by this evolution: for instance, some restrictions of the use of PABX in working places, and some measures against the use of magnetic cards for discriminatory or electronic surveillance purposes.

At the same time, limitations have been imposed on providers of interactive telecommunications services to offer certain services (for instance: market surveys conducted at home), to record information about the customer's habits (such as choice of TV programmes), or to sell information collected from the consumers in the context of these new services.

The CNIL has also focused its attention on the risks arising from the use of networks for collecting and distributing personal information. Therefore, the use within the public sector of a common personal identification number (security social number, identity card number), which facilitates the interoperability of data bases, has been carefully controlled, particularly in the Health and Social Security, and Police and Secret Services sectors. The bill authorizing the existence of a national identification number, has been abandoned under the pressure of the CNIL. Finally, the sectorial approach developed by the French commission and founded upon "simplified norms", defined in cooperation with the sector and available for this sector, is note worthy.

To summarize, despite the weak but increasing interest of the French population in the problem of privacy (cf. the statistics published by the CNIL: there have been only 4,419 complaints in five years, and only two judicial decisions), the CNIL action is viewed as flexible and effective since it takes into account technological evolution.

3.2. The Citizen's Right to Obtain Information

The dissemination of information considered as a tool for a more transparent and convivial society constitutes the aim of different public actions. In this respect, the MINITEL experience has to be pointed out. Nevertheless, we will analyze the MINITEL phenomenon in the context of the French Communication Order (*infra*, 3.3.). One other major action has to be considered in this respect: the Freedom of Information Act (1978).

If, traditionally, administrative secrecy has been seen as a way to improve the efficiency of administrative work (provided that it ensures the confidence of the public in fair information), the purpose of French Law dated 17th July 1978, "bringing various improvement measures between the public administration and the public", is rather to assert the right of everyone to have access to the information held by the public sector.

In principle, according to this law, all public sector information is accessible to everybody without any special reason needing to be given with the exception of particular information (interests of national economy, national security, privacy or business secrets). Like other Access Laws existing in nine OECD countries (including USA, Canada, The Netherlands, Sweden and Norway), the French Act intends to ensure the transparency of the public administration's activities and decisions. In this way, it provides citizens with the means to understand and, possibly, to dispute the content or the motivation of an individual or collective administrative decision. So, a better balance between the information powers of the citizen and the State can be reached.

It is obvious that the French legislator only sought an improvement in the relationship between the public administration and France's citizens and did not attempt to develop the information market (information being considered as a good with economic value). New regulations like the one relating to the INSEE records have granted the public sector with a legal basis for selling information in competition with the private sector.

3.3. The French "Communication Order"

The ISDN networks will lead to the distribution, through the same channels, of the telecommunications services and traditional audiovisual programs (TV, radio). It will become increasingly difficult to establish clearly the distinction between these two kinds of activities. That is why the French Parliament has decided to prescribe and submit both to common principles and to a sole authority: the CNCL (Commission Nationale de la Communication et des Libertés).

In this context, it must be noted that the respect of civil liberties has been founded upon the constitutional principles governing the press (freedom of expression, plurality of opinions) and upon a disenrolling of the public monopoly.

It is obvious that the development of civil liberties is not the sole purpose of this policy which is considered as a tool for ensuring a free market for the French telecommunication industry.

To have a complete idea of this new telecommunication order, we will analyze, firstly, the particular problems arising from the Minitel experience

and, secondly, the principles laid down by the "Freedom of Communication Act" dated September 30th, 1986.

3.3.1. The Minitel experience

Born at the beginning of the '80s and strongly supported by the French government for ensuring a maximum development of the French telecommunication industry, the Minitel experiment was officially intended to promote a better relationship between the citizen and the public administration and therefore to permit the creation of a more convivial society at a local level. Videotex interactive services extend beyond these initial purposes and are developed more and more by private enterprises for electronic publishing, electronic mail, access to data bases, teleshopping, etc.

The legal framework for providing such interactive services is characterized by the principle of individual freedom combined with the minimum administrative requirements considered as mandatory to ensure the plurality of opinions.

It is interesting to underline that the legal regime has until now focused on the similarities between interactive media and traditional media (like the written press and audiovisual activities). Therefore, the legal provisions enacted by the December 13th 1985 Act, September 30th 1986 Act, January 4th 1985 Decree and April 6th 1987 Decree set up a regime imposing specific duties on large public telematics services providers. For instance, each service provider, in the context of the MINITEL experiment, has to:

1. notify the existence of the service and transmit to an administrative authority (the CNCL, see *infra* 3.3.2.) information about it;
2. allow a right of reply to the person concerned;
3. provide a clear separation between the editorial and financial functions of the service;
4. give information to the user about the tariff, the name of the editor and publisher and also a clear identification of the advertisements;
5. store a copy of the messages sent by the provider;
6. not interfere with electronic messages which are to be considered private correspondence.

This legal framework has been built up progressively under the initiatives of a Commission specially nominated for ensuring the follow-up of the development of these new services, the "Commission du suivi des expériences télématiques destinées au public". It is important to emphasize the importance of the so called "soft" law enacted by this commission to avoid the heaviness characterized by the enactement of Decrees or Acts using the traditional legal approach The flexible regulatory framework provided by the Commission enables efficient control of the development of the Videotex services because these services use a technology in ermanent evolution.

3.3.2. The "Freedom of Communication Act"

This Act asserts the principle of the freedom of communication. To enforce this principle, it set up an independent commission with a very broad competence.

The *Freedom of Communication Principle* has two meanings: firstly, the freedom to establish and use telecommunication equipment; secondly, the freedom to operate, manage or utilize telecommunication services, including audiovisual communications (that is to say, large public TV or radio programmes).

The Act intends to combine, on the one hand, the "Freedom of Communication" principle as defined by art. 11 of the Human Rights Declaration and, on the other hand, certain other principles, like public order, plurality of opinions and freedom of individual choice. "The goal to be achieved is that TV and radio listeners and watchers ... are both able to exercize their freedom of choice without either private interests or public authorities imposing their own decision-making, nor their being rendered solely a market object" ("L'objectif à réaliser est que les auditeurs et les téléspectateurs... soient à même d'exercer leur libre choix sans que ni les intérêts privés, ni les pouvoirs publics puissent y substituer leurs propres décisions, ni qu'on puisse en faire les objets d'un marché").

With regard to the audiovisual communications, the combination of these various principles is insured by a legal framework substantially similar to that applicable to the press. So the right of reply (1987 Act), the principle of the transparency of the financial means (1986 Act), the duty to nominate an independent editorial board (1985 Act), the extension of the Journalist's statute (1987 Act) and the control of concentrations (1986 Act) are also applicable to audiovisual communications.

Concerning other telecommunications services, a bill has been laid down before the Parliament during 1987 by the previous government: a strong liberalization for providing value added services was proposed, despite the maintenance of the present State monopoly on the basic network of the technical infrastructure. According to the bill, each private network using the infrastructure ought to be authorized by the CNCL and ought to respect certain conditions dependent upon the requirements of interoperability and public order.

The bill had been withdrawn by the previous Government, under the request of the CNCL, denouncing the absence of any provision asserting the principle of competition. Presently, a decree dated September 24th 1987 provides liberalization for the provision, through leased lines, of telecommunication services offered to third parties.

The creation of an independent authority, the CNCL, to which very important competence is granted, is definitively the second major option of the French Telecommunication Order. Indeed, the 1986 Act grants to the CNCL the power to regulate and control the whole telecommunication sector. For instance, the allocation of frequencies, the authorization for setting up telecommunications networks or providing audiovisual communications are all within its competence.

The goal pursued in establishing an independent authority, which is clearly distinguished from the governmental administration is surely, firstly, to provide freedom for private operators in a competitive market and, secondly, to ensure the respect of the main constitutional liberties.

To summarize this brief overview, there is a common denominator in all the topics characterizing the French legal approach. By various regulations, independent authorities, like the "Commission du suivi des expériences télématiques", the CNIL and CNCL, are granted the competence for regulating the challenges arising from developments with regard to civil liberties. Therefore, public choice related to the distribution, dissemination and provision of all sorts of information (including TV programmes), through telecommunications channels progressively defined not by the constitutional authorities, like Parliament or Government, but by independent authorities, whose management takes into account different, and also sometimes opposing, interests.

4. The German Case

4.1. The Empirical Situation

Information and communication systems in the Federal Republic of Germany (FRG) illustrate three outstanding features, the combination of which makes the West German case a good example for learning:

- a centuries-old bureaucracy and a very effective economy, both contributing massively to citizens' and consumers' files;
- highly sophisticated information and communication systems both in the public as well as in the private sector, mainly in "sensitive" fields;
- a well-established pre-democratic tradition of "numbering people".

Though some countries are more advanced in specialized areas, the West German reality as a whole gives a realistic impression of the opportunities and risks for civil liberties in the computer age.

4.1.1. Convergent Technology

Before sketching the main problem areas, it is important to bring to mind the present stage of information technology development: the characteristic feature of this process is a gradual convergence and interlocking of entire families of information technologies which were hitherto isolated:

- the data processing technology (computers, PCs, microprocessors) applied in business and administration since 1960;
- the text processing technology ("bureautics") amalgamating since 1975;
- the data transferring technology (telecommunication): combining since 1980;
- along with complementary technology in all phases:
  - . data collecting technology (sensors, receptors)
  - . data storing technology (microfilm, tapes, ROMs, optical discs)
  - . data multiplying technology (traditional media; copying machines; printers, etc.).
  - . as well as other (e.g. input/output) technology.

The present interim stage adds various *combinations* of information technology, such as:

- interactive videotex = telephone + computer + TV screen; the German version of the U.K. Prestel system;
- cards with identifiers, machine readers and teletransmittors to background computing;
- computer and telecommunication networks;
- not to forget the different "bridges" to the old machinery of manual labour (effectors, CAD/CAM/CIM, computerized chemistry and atomic energy).

The result will be a networking of all technologies, including old manual work industry and new biotechnology, and including any data about anything (including individuals, groups, financial and personal relations, and institutions). The result will be a "convergent technology".

4.1.2. The Main Problem Areas: The German Case

The problem areas in the field of civil liberties are the same in all highly industrialized countries. First, in the technological field, *as regards public administration*, one can denote: security and intelligence information systems and social welfare information systems; a German "speciality" often imitated by other countries is the citizens' registration system, together with public identifiers. *In the commercial area:* there are personnel information systems and chip cards. In both the public arena *and* private households, there are "new media", teleservices, and telecommunication networks.

Public Sector Information Systems

The process by which the public sector has been underpinned by numerous information systems, including data banks has levelled off - with the exception of the security and welfare sector. All areas susceptible to automation, given a reasonable cost-benefit ratio, have been automated. The next innovatory stage is the integration of work-place office automation and the introduction of digital telecommunication with a view to integrating these systems into only a few networks. This process of integration started for the security sector in 1981, followed by the general public sector in 1983.

To illustrate this trend, amongst others, the example of the "Sozialinformationssystem der Bundesrepublik Deutschland" ("Social Data Information System of the Federal Republic of Germany") can be used. This system is designed to serve the information and planning purposes of the social insurance system (health insurance, old age pension insurance, accident insurance) as well as of the labour and social services' administration (unemployment insurance, public rent allowances, student grant system, and other welfare areas).

Not only does it contain the most comprehensive data collection that a state in either the East or the West has ever assembled about its citizens; it is by the same token the biggest and most up-to-date system in the Federal Republic - which easily explains the interest shown by security and other authorities in these data stocks. Its complex organization defies even expert understanding. Distributed among hundreds of data banks and containing

thousands of personal data files, they are linked together by a convoluted system of manual and automatic data communications (in part prescribed by legal provisions) and open to access by several thousands of participating authorities. They depict a data profile of an estimated 95% of the population, i.e. all employees and their family members. This is not only done to fulfill social purposes, but also (under certain conditions which may be easily satisfied) to benefit the security authorities and research and planning purposes.

This system of systems could turn out to be the most hazardous system of the Federal Republic, if there were not other, even more dangerous, developments to be reported. There is now:

. a 12-digit Social Security Number (SSN)
. a workers' and employees' card, machine-readable, with SSN: no work without card, but heavy punishment;
. a health insurance card, machine-readable, with SSN;
. a health insurance account: a file containing all welfare measures, doctors, receipts, health measures, cures, therapies of the insured, his/her children, etc., and, naturally, the SSN.

And all this goes into the hands and files of thousands of authorities! What should give the public reason for concern is the fact that these measures are (hopefully unconsciously) a replica of Nazi plans (which partly failed through lack of information technology). The future status of this gigantomanic data project has not yet been decided.

Of course, such a file of files needs a potent identifier. The general numbering of citizens by a *personal universal identifier* originally envisioned in 1944, and again in 1960, with a view to creating a residents' information system (also available in Belgium, Sweden or Israel), was dropped as unconstitutional. But it was replaced by the decisively more effective *machine-readable identity card* and *machine-readable passport*, one of which must be carried by every citizen in public, as well as a few other sectoral identifiers, such as the above mentioned social security number. This first mass-control technology of any civilization in the East or West does not function merely as an identity card but is connected via an automatic reading device with built-in telecommunication to further personal data files in other public security authorities which are again connected with other administrative files. Add to this that the police authorities are in charge of the registration offices (and their files) in about half of all the individual FRG states and it makes the social relevance of this system obvious.

Business Sector Information Systems

In the *commercial sector*, two groups of business information systems should be distinguished:

- information systems designed for the internal purposes of the relevant business enterprise;
- information systems set up for external commercial use of information as a "merchandise".

Personnel Information Systems: these were originally set up to rationalize the personnel system and to facilitate planning. Personnel data

deeply modified

processing is now spread amongst thousands of files and dozens of subsystems to the most diverse of secondary uses. But personnel information systems do not "stand alone". Presently the automation of various secretarial activities work ("text processing") is being added; using "in-house" or "local networks" (i.e. firm-owned communication networks). These activities are increasingly monitored with respect to the individual work-place and the individual employee (or groups thereof). These systems, too, are personnel information systems, and capable of comprising working units distributed on several continents to a "virtual" information unit. Such "distributed" systems cannot guarantee citizens' or employees' traditional legal safeguards against unlawful use, i.e. for purposes other than originally held.

With regard to the *Information Industry and Chip Card,* already by current practice, any information, inclusive of that on individuals, is an appreciated immaterial "good" for credit agencies and detective agencies; of late it has also becomes so for market research, public opinion research, publicity firms, and innumerable private research institutes. They all increasingly draw on facilities of text and data processing as well as on those of telecommunication with a view to bettering their market position in quantitative and qualitative terms. The external utilization (sale) of originally internal data on customers and employees has also to be seen in this context.

There are, moreover, information service enterprises (e.g. credit reporting agencies) which are gathering or processing personal data on the credit standing or business behaviour of customers and employees for insurance/banking or other purposes. Thus we have:

- agencies gathering data;
- software houses (i.e. producers of computer programmes);
- commercial computing centres (selling EDP capacity);
- operators and hosts of commercial telecommunication networks (offering the services of tele data transmission);
- finally, world-wide computer networks (which in part are in a position to offer all the functions mentioned and, in addition, the services of documentation services and data banks).

The banking industry promotes a technically more advanced version of the "machine-readable identity card" for commercial aims. It does so for several reasons: first, it needs a simple means to code or decode the financial and informational transactions of individuals using technology-supported information systems; second, it wants to use these users' transaction data for marketing purposes; third, it gets better connections to "new media" use of households; fourth, data protection legislation hinders commercial use of the public identification card. The solution to this "bundle of wishes" is an "intelligent" device named a "smart" or "chip card" furnished with one or two microprocessors, an autonomous energy supply, a telecommunication interface, and ample storage room for personal data and encryption software.

"New Media", Tele Services and Networks

All these manifold developments overlap to create a tangled bundle of knots and wires. This overlapping endangers citizens' liberties far beyond any hope for a simple cure to the problem. But this is not the whole problem; entrance into private households is to be accomplished by "new media", tele services and networks.

"New Media" is a misnomer hiding compounds of advanced computer technology with "old" information technologies combining the facilities and problems of both. The term "New Media" conceals the fact that they imply an amplification of the traditional "old media" (print, film, radio, TV) in a double sense:

- by data processing (the computer is the only information technology capable of actively manipulating information whereas the old media are only capable of passively multiplying and transmitting them);
- and by telecommunication (satellites and broad-band transmission are capable of extending the traditional capacity of wire or wireless transmission and multiplication by several decimal exponents).

A good example is the current interactive videotex (German Bildschirmtext = Btx; U.K.: Prestel; Canada: Telidon; France: Télétel). Originally videotex was meant to become an entrance to the tele computer world for anybody: for firms, authorities, households. It gives computer capacity or computerized information upon a phone call to the screen of the user. It was meant as an omnipurpose system which may be put to any desired information processing and distributing purpose, be it internal or external, particularly as an efficient instrument of rationalization in both business enterprises and authorities. But, fortunately, it was a flop; it was a monster cross-breed of latest computers and oldest copper-wire telephone, with inadequate precautions against intrusion into the citizens' private sphere and/or commercial/political abuse of data. Its use by customers is followed by subsequent feedback information on the attitude of the user transmitted by phone, for the purposes of accounting, marketing, and control in general.

Interactive videotex will be one of many teleservices of the future telephone network. More than a telephone in essence, it is a distributed macrocomputer on which as many functions as programs may be run on or over it. This overall international multifunctional "Integrated Services Digital Network" (ISDN) will be a network for all purposes including television, when using glass fibres (beginning circa 1988). The legal problem lies in the fact that a digitalized (that is computerized) telephone network in its legal sense is no longer a telephone but a programmable (and hence controllable) active computer system. In addition it provides the infrastructure for connections with any other other technology in any place such as, for instance, teleworking places in households.

The international telecommunication and computer networks which are now operative will put literature, patents, and other text and data banks at the disposal of financially powerful customers at a fraction of the postage and copying costs paid so far. They will merge with ISDN or their equivalents in the near future in a computerized general information and communication infrastructure.

In political or economic terms, the following three subsystems of society - business, political, and private sphere - which were hitherto more

or less separated will be superseded by a supersystem integrating them in an informational superstructure. Privacy and civil liberties' problems will superseded, too. How this networked "distributed problem" will be dealt with is unknown.

4.2. The Legal Answer to the Technological Challenge

In the legal field we find another West German peculiarity which tends to be imitated in other highly industrialized countries: an extensive data legislation which is partly out of democratic control.

4.2.1. Unlawful Law

One "German" phenomenon is the peculiar inclination of technocrats not to give up their unconstitutional activities but to legalize them by legislation. This is a bad example which is beginning to find imitators. The most urgent problems regarding the infraction of civil rights consist of two overlapping legislatory activities. First, the facts:

The new Bonn government has installed a whole bundle of (state) security laws under the pretext of terrorism: the identity card law, which states that it is everyone's duty to present this machine-readable card or passport at any time to any policeman; a passport law, installing a machine-readable passport; an amendment to the penal procedure act giving security forces the permission to 'drag' or 'trawl' whole districts and search *any* person found[9] there and store their data, and - in many cases - their fingerprints; an amendment to the traffic regulation statute giving security forces additional online access to 25 million car drivers' files, thus combining the knowledge of ZEVIS[10] with INPOL and inhabitants' registration files.

A second bundle of legislation is on the way: the enabling of and, on demand, the duty of *any* public authority to denounce the anti-statal activities of any citizen or foreigner to the secret services; the duty to cooperate and to exchange data between police and secret services, which was forbidden by the allies after 1945 in order to prevent a new Gestapo ("Geheime Staatspolizei"= secret state police); all this, together with additional restrictions of the constitutional right to utter public opinion in the form of demonstrations.

These legislative changes must be seen in the context of the above mentioned activities in the social welfare sector. A planned amendment to the Federal Data Protection Act takes new online connections between administrative information systems out of democratic control. The failure of repeated attempts to enact a Freedom of Information Act is quite

---

9 This is the so-called "Schleppnetzfahndung" (trawler search).

10 ZEntrales Verkehrs-Informations-System = Central Traffic Information System. This online connection is apparently unconstitutional, i.e. illegal, according to Brinckmann 1987a.

opposite to the ancient administrative principle of "office secrecy" which is still effective.

No wonder that these activities in their interaction raise fear amongst those who remember the National Socialist '30s. But certainly this is *not* a new Fascism. The reasons behind this conservative power-play, which endangers the young West German democracy, is an "inner rearmament" against the political consequences of a rapid decrease in social security and an increase in state military expenditure. Officially it is meant to fight terrorism, but in reality it enforces authority against civil disobedience. This is a new phenomenon in Germany (cf. the public census affair in 1983 and 1987).

4.2.2. Information Law as the Law Relating to the Industrialization of Intellectual Work and Communication

Information (or data) law deals with the social control of information systems *and* of their social effects. Whereas the old technologies produced material goods and services, the new ones "produce" information and communication, i.e. power, in the sense of an opportunity to influence the behaviour of people and other objects.

This difference in character is reflected in the law. There is only one new field of law, the law on electronic data processing (EDP-Law), also called information law or, more accurately, termed information technology law or *data law*. Data law is the legal equivalent of informatization. In contrast, solutions to the problems of the industrialization of manual *and* intellectual works have so far for the most part been found within the context of traditional labour law (mainly that of labour-management relations and staff representation) as well as the law relating to the "environmental" effects emanating from macro technologies: the latter are solvable presently only by political means.

In this new discipline of data law, several branches have come to the fore: the Law on the Protection of Personal Data (data protection law) takes the most prominent position, in particular the statutes on data protection enacted by the Federal Republic and its individual states (including West Berlin, though, it should be noted, the law of the occupation powers takes absolute precedence). Its main features are:

- strict distribution of data to firms and administrations according to the minimum they need for their duties;
- data protection commissioners to help citizens in the jungle of public administration data systems, and (very small and, hence, helpless) data protection offices, in the commercial data field;
- the principle of informational division of powers in some of the Länder's data protection statutes as a consequence of the increased information power of administrations.

The statutes regarding the organization of information systems obtained in the respective individual states lay the legal basis for administrative information systems and computer centres; for instance to the INPOL-system referred to above, or for social security data banks, or in the field of statistics.

Special statutes deal with individual technologies of information and communication; they give provisions for
- the gathering of data: e.g. the statutes on the different machine-readable identity cards;
- the transmission of data: executive orders regarding the gathering and transmission of data between employers and public social insurance agencies;
- for "new media and telecommunication: the statutes on cabling and on Btx of the Länder as well as the Telecommunication Provision for ISDN of the German Federal Post Office.

Special provisions in traditional statutes provide a legal basis for supporting and limiting the use and transmission of information technologies in the various social realms (medicine, security authorities, administration, and many others).

Provisions aimed to promote technological transformation in the administration and/or to facilitate it legally are:
- regulations on the procedures of technological development;
- regulations on the adjustment of traditional manual procedures;
- even regulations on how to formulate legal norms so that they can easily be automated.

The churches have enacted data protection regulations too for rather questionable reasons (to get access to registration files to facilitate "church tax" payment).

It is worth emphasizing that all these statutes - in addition to their primary goals - also serve the function of indirectly securing the liberties of the citizen by
- controlled distribution of information;
- additional entitlements to information;
- embedding information systems into the organization of the state according to the principles of the constitution (by organizing statutes);
- special provisions on specific technologies and their implications.

Hence it is wrong to confine the topic of data law to data protection law. The law on data protection has the function of organizing, by distributing data and information power. The remaining species of data law have a "citizen-protective" function.

4.3. Limits and Changes of Legal Regulations

4.3.1. Data Protection is Correct Systems Design more than Data Protection Law

Data protection *is not a question of law alone*. A well-designed computer system needs few extra data protection measures, if designers are aware that data protection is a tailor-made bundle of technical, organizational, and legal measures. Besides, data protection "the day after" is far more expensive. We prefer systems' protection, which we believe will be effective, in terms of costs as well as regarding the citizen.

This is true for individual information systems. It is even more true for the whole of society. There must be democratically accepted principles (of

transparency to public control, or of institutionalized help to the citizen and employee) which must be obeyed, if data protection is to be more than an excuse.

4.3.2. Data Protection is not enough

Data protection is merely "negative". It prevents the people affected from being damaged by data (use). It is "defective" too, since it does not help against rationalization risks; it is restricted to informatization problems. Macro-technology risks of megasystems are beyond its scope.

We need a "positive" complement. We need "humane" systems. That is a problem of construction far more than of mere prevention. But what is "humane"? In practice, it is of no use to construct philosophical systems in order to derive "correct" criteria, though in this field there is much research is still to be done. Instead, we should ask the people affected a few questions:

First: do we need this system or can we do something better without a computer?

Then we should ask the user at the workplace:

- Are (hard-, soft-, orgware) ergonomic requirements fulfilled?
- Do you want to keep, improve or change your qualification?
- Do you propose another labour organization, perhaps to improve the quality of your labour ?
- Under which conditions will there be no loss of workplaces?

There are always several people in the firm who are indirectly affected:

- What are the short or long range effects of reorganization due to information or communication technology introduced elsewhere that you fear or want to come?
- What necessary arrangements with the affected users should you propose in order to get a result in your favour?

Finally to the modelled, and hence possibly controlled, citizen:

- To the employed: How to reduce or even avoid unnecessary data or programs on personnel? What is the interactive effect of rationalization and modellification personally and in your workplace?
- Customers, clients, third parties in general: Do we take over our responsibility for them? How can we organize the system in a way that they (a) can participate in the system's design, and (b) are capable of executing their constitutional right of information self-determination?

These questions do not solve the problem. They just indicate a direction in which to go. It is a question of correct design, and of better education of the worker and the citizen. Altogether, this is the most urgent research problem in this field.

SOURCES

Bull, H.P. [1984], *Datenschutz oder die Angst vor dem Computer*, München: CH Verlag Beck.

Burkert, H. [1982], Institutions of Data Protection: An Attempt at a functional Explanation of European *Computer Law Journal*, 3, 167-188.

Burkert, H. [1985], *Datenschutz und Informations - und Kommunikationstechnik: Eine Problemskisse*, Bonn: GMD Publications.

Burkert, H. [1988], The Law of Information Technology - Basic concepts, *D.u.D.*, 8, 383-387.

Commission Nationale Informatique et Libertés (CNIL), [1988], *Dix ans d'Informatique et Libertés*, Paris/La Documentation Française.

CNIL, *Rapports d'activité de la Commission Nationale de l'Informatique et des libertés*, Paris: La Documentation Française (each year, since 1980).

Froystad, D. [1984], *Data Protection in Pratice: Identifying and Matching Element*, Oslo: Complex.

Holvast, J. [1986], *Op weg naar een risicoloze maatschappij ?*; Den Haag: Academic Service

Informationsgesellschaft oder Uberwachungsstaat, [1984], Symposium der Hessischen Landesregierung, Wiesbaden: Starck'sche Druckereigesellschaft m.b.H..

Perry, Ph. [1987], Data Protection update, *Computer Law and Practice*, 4, 39-40.

Poullet, Y. [1987], Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information, *Droit de l'Informatique*, 4, 22-227.

Pounder, C.N.M., Kosten, M., Papadopoulos, S., Richard, A, [1987], *Managing Data Protection*, London CIPFA - C.C.S..

Rankin, T.M. [1986], Business secrets across international borders: one aspect of the TDF debate, *Computer Law and Practice*, 2/4, 106-118.

Savage, N. and Edwards, C. [1984], The Data Protection Act 1984, *The Journal of Business Law*, 320-325.

Schneider, J. [1984], Datenschutz und New Medien, *N.J.W.*, 390-394.

Selmer, K. [1988], Data Protection Policy Trends, *T.D.R.*, 10, 19-25.

Steinmüller, W. [1983], Information Technology and Information Law, *Information Age*, 5, 39-46.

Steinmüller, W. [1984], Consequences of Information Technology, *Information Age*, 6, 163-177.

Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, Bönn/ Bundestags-Drucksack (each year, since 1978).

~~TO BE COMPLETED~~

~~Missing citation: BRINDEMANN [1987]~~