Information Technologies and Civil Liberties, Landscapes of an Information Society

MICHAEL, James; STEINMULLER, Wilhelm; Poullet, Yves

Publication date:
1988

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

mai 1988.

III

INFORMATION TECHNOLOGIES AND CIVIL LIBERTIES

J. MICHAEL - Y. POULLET - W. STEINMULLER.

1. "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 about 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 technologies, at the very least, greatly increase 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.

2. Two particular legal developments are relevant to information technologies and civil liberties/rights, usually described an 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) to make 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 taht 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 technologies (although some data protection statutes are).

3. 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 (offentilighetsprincip). 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 (to use its more common name), 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 at a near exponential rate.

4. This chapter, 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 (chap. I and II). Yves POULLET describes French legislation on data protection and open government together with related developments such as Minitel (Chap. III). Wilhelm STEINMÜLLER analyses the civil liberties issues presented by information technologies in the Federal Republic of Germany and concludes the chapter with a caution on the limits of legal regulation (Chap. IV). The emphasis throughout is on the legal solutions attempted to the problems of civil liberties prested by converging information technologies; 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

5. Although the right to privacy is problaimed 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. A similar case challenging a similar law in the Republic of Ireland is now pending.

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 th newx international markets in information. As regards the position of the EEC, we want to underline the manifest, trend to undermine national civil liberties' legislation on data protection by "Common lowest level" regulations, for economic reasons.

---

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

6. 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 good 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 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 Guildelines. 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

7. 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 byu judicial creativity. The right to privacy in Anglo-American law developed through both judgemade case law and legislative statutes before it emerged as a human right in international law, and is the path of development with wich this writer is most familiar.

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 generally be recognized 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.

8. 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 hads 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 etchings, rather than the original etchings themselves (which would have been

---

2 41 English Reports 1171.

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 injuction 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 envolve 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 dit 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 1690. 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 of embarrassing private facts, presenting an individual in a false light, and appropriation of a name or likeness [3].

9. 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 specitif 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.

10. In Ireland the right to family privacy is established by Article 41.1.1 of the Constitution, and in Mc Gee v. Attorney-General [7] it was held to be violated by a law

---

3 48 California Law Review 383

4 381 U.S. 479

5 381 U.S. 479

6 410 U.S. 113

7 1974 Ir. R. 284

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, as successful campaing was mounted to amend the constitution to ban abortion.

11. 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 monetheless is very similar to Roe v. Wade [8], the Supreme Court of Canada has recently held the Canadian law regulating abortion to be unconstitutional. Meanwhile, the U.S. Supreme Court has resiled somewhat, holding in Bowers v. Hardwick[9] that a state law making homosexual (and perhaps some heterosexual) acts criminal dit not violate the right to privacy.

12. 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 applying to both manual and automated records, but it is more narrow in applying only (oral least 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 Zeland has a technology-specific law regulating the police national computer, and a relatively the police national computer, and a 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 mesure of information about people. The is much to be done, and always the danger that symbolic reassuring legislation can do more harm than good : but there has been a beginning.

3. ROMAN LAW TRADITION: THE FRENCH CASE

13. Under this title, only the French case will be considered, one reason being that the laws embracing the problematic : "Information Technologies 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 original compared with the German or English one. In my opinion, the French regulatory framework is focused very much on the citizen's right to obtain information from the public sector (4.1.) with a view to protecting the same citizens against misuses of information by public or private sectors (4.2.).

A second original feature of the French case is to create a legal framework anticipating the convergence of the medias, allowed by the new technologies of telecommunication and to submit the different forms of communications including

---

8 92 L. Ed. 140 (1986)

9 (1981) Series A, Vol. 45

audiovisual programms to global solutions : someone speaks about the creation of a "Communication order" (ordre de la communication) (4.3.).

3.1. Computer and Liberties : Debate and Trends

14. Ten years ago, January 10th 1978, the French Parliament enacts a 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 : "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 Computer and Liberties (C.N.I.L.), which was created by the Act, have made a number of suggestions in respect of new services created by the NTI evolution. For instance, some restrictions of use of PABX on working places, some measures against the use of magnetic card for discriminatory or electronic surveillance purposes have been ruled by the Commission.

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

The C.N.I.L. has also focused its attention on the new risks arising from the use of networks for collecting and distributing personal information. Therefore, the use within the public sector of common personal identification number (security social number, identity card number), which facilitates the interoperability of data bases, has been carefully controlled, particularly in the sectors "Health and social security", "Police and Secret Services" and the bill providing the existence of a national identification number, has been abandoned under the pressure of the C.N.I.L..

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 problematic of the Privacy (cf. the statistics published by the C.N.I.L.: only 4.419 complaints in five years, only two judicial decisions), the C.N.I.L. action is viewed as flexible and effective since it takes into account the technological evolution.

3.2. The citizen's right to obtain information

15. 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, 4.3.).

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 efficiency of the administrative work provided that it ensures the confidence of the public which has to give fair information, the purpose of the French Law "portant diverses mesures d'amélioration entre l'administration et le public", dated 17th July 1978, is to assert, in a countrary way, the right of everybody to have access to the information held by the public sector.

16. In principle, according to this law with the exception of certain information (interest of national economy, of national security, of privacy or business secrets), all public sector information are accessible to everybody without any special reason having to be given. Like others Access Laws existing in nine OECD countries (USA, Canada, The Netherlands, Sweden, Norway, ...), the French Act intends to ensure the transparency of the administration's activities and decisions. In this way, it provides the citizens with the means to understand and, possibly, to dispute the content or the motivation of an administrative individual or collective decision. So) a better balance between 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 administration and citizens and dit 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 to the public sector a legal basis for selling information in competition with the private sector.

3.3. The French "communication order"

17. The ISDN networks will lead to the distribution, through the same channels,of the telecommunications services and the classical audiovisual programs (T.V., radio) and 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 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, first, the particular problems arising from the Minitel experience and, secondly, the principles laid down by the "Freedom of Communication Act" dated from september 30th 86.

3.3.1. The Minitel experience

18. Born at the beginning of 8O' and strongly supported by the French governement for ensuring a maximum development of the French telecommunication industry, the Minitel experiment intended officially to promote a better relationship between the citizens and the administration and therefore to permit the creation of a more convivial society at a local level.

Videotex interactive services go now beyond these initial purposes and are developed more and more by private enterprises for electronic publishing, electronic mail, access to data bases, teleshopping, etc...

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

It is interesting to underline that the legal regime is until now focused on the convergences or similarities between that media and the classic media, like 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 imporing some duties on a lage public telematic 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 C.N.C.L., see infra 4.3.2.) certain informations thereabout;
2. allow a right of reply to the persons;
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 ot the advertisements;
5. store copy of the messages sent by the provider;
6. not interfere with electronic messages which are to be considered as private correspondance.

20. This legal framework has been built up appointed 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 underline, in a first time, the importance of the so called soft law ruled by this commission (deontological norms, cahier des charges) in order to avoid the heaviness characterizing the enactment of Decrees or Acts, following the classical legal approach. The souple regulatory framework, provided by the Commission, does afford to control efficiently the development of the Videotex services because these services use a technology in permanent evolution.

3.3.2. The "Freedom of Communication Act"

21. This Act asserts the principle of the Freedom of Communication. To enforce this principle, it sets up an independant commission with a very broad competence.

The Freedom of Communication Principle has two meanings : firstly, the freedom for establishing and using telecommunication equipements; secondly, the freedom for operating, managing or utilizing telecommunication services, including audiovisual communications that is to say, large public TV or sound programmes.

The Act intends to combine together, on the one hand, the "Freedom of Communication" principle as defined by art. 11 of Human Rights declaration and, on the other hand, certain other principles, like public order, plurality of opinions and freedom of individual choices. "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 sector. So the right of reply (1987 Act), the principle of the transparency of the financial means (1986 Act), the duty to nominate an independant editorial board (1985 Act), the extension of the Journalist' statute (1987 Act) and the control of concentrations (1986 Act) are also available for audiovisual communications.

Concerning other telecommunications services, a bill has been laid down before the Parliament during 87 by the previous government: a strong liberalization for providing value added services was proposed therein, notwithstanding the maintenance of the present State monopoly on the basic network that is to say, the technical infrastructure ? According to the bill, each private network using the infrastructure ought to be authorized by the C.N.C.L. and to respect certain conditions infered from the requirements of interoperability and public order.

The bill has been withdrawn by the previous Government, under the request of the C.N.C.L., denouncing the absence of any provision asserting on the competition principle. Presently, a decree dated from September 24th 1987 provides only liberalization for providing, through leased lines, telecommunication services to be offered towards third parties.

22. The creation of an independant authority : the setting up of the C.N.C.L. (Commission Nationale de la Communication et des Libertés), whereto very important competence is granted, is definitively the second major option of the French Telecommunication Order. Indeed, the 1986' Act grants to the C.N.C.L. the power to regulate and control the whole telecommunication sector. For instance, the frequencies allocation, the authorizations for setting up telecommunications networks or providing audiovisual communications are within its competence.

The goal pursued by establishing an independant authority, clearly distinguished from the governmental administration is surely first to ensure a truly freedom for private operators in a competitive market and, secondly, both to control the respect of the main constitutional liberties.

23. To summarize this brief overview, one wants to point out a common denominator of all the topics characterizing the French legal approach. By various regulations, independant authorities, like "Commission du suivi des expériences télématiques", C.N.I.L. and C.N.C.L., is granted to the competence for regulating by soft laws the challenges arising from the NTI developments in regard to our civil liberties. Therefore, the public choices related to the distribution, dissemination and provision of all sorts of information (including classic T.V. programmes), through telecommunications channels are progressively defined not by the constitutional authorities, like Parliament or Government, but by independant authorities,whose management allows to take into account different and also sometimes opposite interests.

4. THE GERMAN CASE

4.1. The Empirical situation

24. Information and communication systems in the Federal Republic of Germany (FRG) show 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 private sector, mainly in "sensitive" fields
- a well-established pre-democratic tradition of "numbering people" since the Third Reich accepted elsewhere much later.

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

4.1.1. Convergent technology

25. 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 hitherto isolated:

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

The present interim stage adds various combinations of information technologies, 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 old machinery of manual work (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, including any data about anything including persons, 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 case of civil liberties are more or less the same in all highly industrialized countries. First on the technological field, as regards public

administration; one can denote : security and intelligence information systems and social welfare information systems; a German "speciality" but more and more imitated by other countries is the Citizens' registration systems, together with public identifyers; in the commercial area : personnel information systems and chip cards; for both *and* the "private" households : "New media", tele services, and telecommunication networks.

Public sector information systems

27. As it seems, the process by which the public sector has been underpinned by numerous information systems including data banks, for the time being, has levelled off - with the exception of the security and welfare sector. All areas susceptible to automation, given a reasonable benefit-cost-ratio, have been automated so far. The next innovationary stage now is being reached bythe integration of working-place office automation and the introduction of digital telecommunication with a view to intergrating these systems into a few networks. This process of integration has already started for the security sector in 1981, followed by the general public sector since 1983.

28. 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 developed. This system is designed to serve 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 ever a state in West or East has assembled about his 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 organisation 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 or automatic data communications (in part being prescribed by legal provisions) and opened for access to several thousands (!) of participating authorities, thus depicting by data of an estimated 95 % of the population, i.e. all employees and their family members. This is not only done, it is worth noting, in fulfillment of social purposes, but also (under certain conditions thich may be satisfied easily) for security authorities, research and planning purposes.

This system of systems would turn out to be the most hazardous system of the Federal Republic, if there had not been some more dangerous recent developments to be reported now: the additional installation of a

(1) 12-digit Social Security Number (SSN)
(2) Workers' and employees' card, machine-readable, with SSN: no work without card, but heavy punishment
(3) Health insurance card, machine-readable, with SSN
(4) 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 into the hands and files of thousands of authorities ... What should give reason for public concern is the fact that these measures are (hopefully unconsciously) a

replica of Nazi plans which then partly failed through lack of information technology. The future status of this gigantomanic data project is not yet decided.

29. Of course, such a file of files needs a potent identifier. The general numbering of the citizens by a personal universal identifier envisioned originally 1944, and again 1960 with a view to the use of the resident information system (also available e.g. in Sweden or Israel), was dropped as unconstitutional, but was replaced by the decisively more effective so-called machine-readable identity card and the machine-readable passport, one of which must be carried by anybody in public, and a few other sectoral identifiers, as the above mentioned social security number. This first mass controll technology of any civilisation in East or West does not function merely as an identity card but is connected via automatic reading device with built-in telecommunication to further personal data files of other public security authorities which themselves are connected again 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 individual FRG states to make obvious the social relevance of this system.

Business sector information systems

30. In the commercial sector, two groups of business information systems should be distinguished:
- information systems designed for internal purposes of the relevant business enterprise
- information systems set up to be used for external commercial use of information as a "merchandise".

With regard to Personnel Information Systems: as is well known, information systems of all kinds have been used since the late '50s for the most diverse purposes of business establishments. In this context, the so-called "personnel information systems" are worth noting with regard to the personal liberties. In practice more important are other non-dedicated information systems processing personel data amongst others. Both types comprise ample data not only of the firms' employees (this was the state of the art in 1970) but also of customers, clients, and others. Originally set up to rationalize the personnel system and to facilitate planning, personnel data processing nowadays in bigger firms is spread amongst thousands of files and dozens of subsystems to the most diverse secondary uses.

But personnel information systems do not "stand alone": Presently the automation of various activities of secretarial work ("text processing") is being added; using the currently promoted "in-house" or "local networks" (i.e. firm-owned communication networks). These activities are increasingly evaluated with respect to the individual working-place and the individual employee (or groups thereof). These systems, too, are (viewed in a functional sense) personnel information systems, and are capable of comprising, as in the case of the so-called "multinational" firms, very well working units distributed on several continents to a "virtual" information unit. Such "distributed" systems no longer obey citizens' or employees' traditional legal safeguards against unlawful use, i.e. for other purposes than originally held.

31. With regard to Information Industry and Chip Card: already by current practice, any information, inclusive that on persons, is an appreciated immaterial "good" for credit agencies and detective agencies; of late also for market research, public opinion research, respectively publicity firms, assisted by 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 of 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 data on the credit standing or business behaviour of customers and employees for all insurance/banking or other purposes.

Thus a whole new-type information and communication industry comes up, all of them dealing more or less with personal data:

- 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 functions just mentioned and, in addition, the services of - sometimes dozens of - documentation services and data banks).

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 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 connection to "new media" use of households; forth, data protection legislation hinders commercial use of the public identification card. The solution of this bundle of wishes is an "intelligent" device named "smart" or "chip card" furnished with one or two microprocessors, autonomous energy supply, telecommunication interface - and ample storage room for personal data and encryption software.

"New media", tele services and networks

31. All these manifold developments overlap to an indisentangible bundle of knots and wires. This overlapping endangers citizens' liberties far beyond any hope for a simple cure of the problem. But this is not the whole problem. State and industry want to get a solid technological entrance into private households. This 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 legally deciding 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). It originally was meant to become an entrance to tele computer world for anybody: for firms, authorities, households. For 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 rationalisation both in business enterprises and authorities. But, fortunately, it became a flop, due to being a monster cross-breed of latest computers and oldest copper-wire telephone, over and above with inadequate precautions against intrusion into citizens' private sphere and/or commercial/political abuse of data: Its use by customers is necessarily followed by a subsequent feedback information on the attitude of the user being transmitted by phone, for the purposes of accounting, marketing, control in general.

32. Interactive videotex will be one of many tele services of the future telephone network, which no more is a telephone in essence, but a distributed macrocomputer with as many functions as programms may be run on or over it. This over-all international multifunctional "Integrated Services Digital Network" (ISDN) will be a network for all purposes including television, when using glass fibres (beginning ≈1988). The legal problem, in a nutshell, lies in the fact that a digitalized (= computerized) telephone network in its legal essence is no more a telephone but a programmable (and hence controllable) active but intransparent computer system, which in addition gives the infrastructure for connections with any other bio- or other technology in any place, which for instance means: for as many tele working places as households.

33. Special mention deserves the international telecommunication and computer networks already now operative which will allow to connect all existing information and its technologies within the near future. They will put literature, patents, and other text and data banks at the disposal of financially potent customers at a fraction of the postage and copying costs paid so far. They will merge with ISDN or equivalents in near future to a computerized general information and communication infrastructure.

In political or economical terms: The three subsystems of society hitherto more or less separated - business, political, and private sphere - will be superseded by a supersystem integrating them by an informational superstructure. From another point of view: their privacy and civil liberites' problems will supersede, too. How this networked "distributed problem" could be dealt with is unknown to experts until now.

4.2. The legal answer to the technological challenge

34. In the legal field we find another West German peculiarity which tends to be imitated in other highly industrialized countries (and this is the reason why it is dealt with here): an extensive data legislation partly out of democratic control.

This is on the background of ample legislation in the data protection and other information law field.

4.2.1. Unlawful law

35. A very "German" phenomenon needs some explanation: the peculiar inclination of technocrats not to give up unconstitutional activities but to legalize them by legislation. It should be mentioned in an international survey since it is a bad example beginning to

find imitators. - The most urgent problems regarding civil rights consist of two overlapping legislatory activities. - First the facts:

The new Bonn government has installed a whole bundle of (state-) security laws on the pretext of terrorism: the identity card law, statuing anybody's duty to present this machine-readable card or passport at any time to any policeman; a passport law, installing this machine-readable passport; an amendment to the penal procedure act giving security forces the permission to 'drag' whole districts and search *any* person found[10] and store their data, even - 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 this ZEVIS[11] with INPOL and inhabitants' registration files.

A second bundle is on the way: the allowance and, on demand, the duty of *any* public authority to give denunciation on 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 publicly utter his opinion by demonstrations.

36. This must be seen in contexts of the above mentioned activities in the social welfare sector, a planned amendment to the Federal Data Protection Act does not make topical new technological developments since 1975 but on the contrary takes new online connections between administrative information systems out of democratic control, the failure of repeated attempts to enact a Freedom of information act, opposite to the ancient administrative principle of "office secrecy" which is still effective.

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

4.2.2. Information law as the law relating to the industrialization of intellectual work and communication

37. 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 a chance to influence the behaviour of people and other objects. Novel in principle, therefore, is merely the "informatization", that is the effects of mechanising information and communication, namely the gain of informational power in favour of organisations using these technologies, whereas the remaining effects (industrialization and rationalisation of brainwork and communication, and its macro-technological

---

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

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

organisation) may also be found in manual work and its technical and organizational forms.

This difference in character of effects is reflected in the law: There is only one new field of law, the (very often so called) law on electronic data processing (EDP-Law), frequently also called information law, more accurately however termed information technology law or data law (data protection law would be a part of it). Data law is the legal equivalent of informatization. - By contrast, solutions to the problems of manual *and* intellectual work's industrialization have so far for the most part been found within the context of the traditional labour law (mainly that of labour-management relations and staff prerepresentation), which is omitted here, as well as the law relating to the "environmental" effects emanating from macro technologies: the latter are, basically, solvable presently only by political means.

38. In this new discipline of data law, several branches have come to the fore: the so-called 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, as should be noted, the law of the occupation powers takes absolute precedence). Its main features are:

- more or less strict distribution of data to firms and administrations according to the minimum they need for their duties
- data protection commissioners to help citizen in the jungle of public administration's 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 data protection statutes, as a consequence of the increased information power of administrations.

The statutes regarding the organisation 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 use and transmitting 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 how to formulate legal norms so that they can easily be automated.

The churches have enacted data protection regulations, too - from rather questionable reasons (to get access to registration files as a basis of "church tax" payment.

It is worth emphasizing that all these statutes - in addition to their primary goals - serve also the function of indirect securing the liberties of the citizen by

- controlled distribution of information
- additional entitlements to information
- embedding information systems into the organisation of the state according to the principles of the constitution (by organising statutes)
- special provisions on specific technologies and their implications.

Hence it is wrong to confine the topic of data law on data protection law merely: The law on data protection has a function of organizing, by distributing data and information power, and 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

40. Data protection *is not a question of law alone*. Computer science research has made evidence that a well-designed system needs little extra data protection measures, if designers were aware that data protection is a taylor-made bundle of technical, organisational, and legal measures. Besides, data protection "the day after" is far more expensive. It must be system protection, then it will be effective, regarding costs as well as regarding the citizen.

This is true for individual information systems. It is the more true for the whole society. There must be democratically accepted principles (e.g., of transparency to public control, or of institutionalized help to the citizen and employee) which must be obeyed, if data protection should be more than an excuse.

4.3.2. Data protection is not enough

4.1. Data protection is merely "negative", prevents people affected from being damaged by data (use). It is "defective", too, since it does not help against rationalisation risks; it is restricted to informatisation problems. All the more, 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 no use to construct philosophical systems in order to derive "correct" criteria, though in this field very 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 it better without computer? This is the famous Weizenbaum question which should always be raised at the beginning.

Then we should ask the user at the working-place:

- Are (hard-, soft-, orgware) ergonomy requirements fulfilled?
- Do you want to keep, improve or else change your qualification?
- Do you propose another labour organisation, perhaps to improve the quality of your labor ? - And the most important one:
- Under which conditions will there be no loss of working places?

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

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

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

- Employed : How to reduce or even avoid unnecessary data or programs on personnel ? Which is the interactive effect of rationalisation *and* modellification in your person and working-place?
- 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 (1) can participate in the system's design, (2) are capable of executing their constitutional right of informational self-determination?

These questions do not want to 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, it is the most urgent research problem in this field, in which only a few minor claims have been investigated until now.