Centre for Computers and Law, Erasmus University Rotterdam

Richard De MULDER and Pieter KLEVE

Computer law in the Netherlands

1. Introduction

The field that deals with the legal aspects of automation is usually called „computer law". This is, however, not the only area of expertise in which information technology and law come together. Telecommunication law and media law are related areas. We will not deal with these in this article, although both have gone through a period of turbulent development and the present situation is still unsettled.

The impact of automation on Dutch law, as in Europe in general, shows two tendencies: protection of information technology and protection of data. It is because of the technological pre-eminence of the United States of America that the influence of the legal developments in the U.S.A. on those in Europe has been considerable. In Europe, however, far too little attention is usually paid to the differences in the legal systems of both continents. The EEC has shown a strong interest in computer law. Harmonization of legislation is necessary in a common European market, but sometimes the EEC directives have seemed all too ambitious and too hasty in adopting the American approach.

2. Protection of information technology

The growing interest in the protection of information technology has mainly been shown in the areas of intellectual property and competition law. There have been new developments in the legal approach with respect to the protection of chips, software and databases.

2.1. Chips protection

Just as in case law it was decided that software was a work in the sense of copyright law, in legal literature it was supposed that the topographies of semi-conductors – the three dimensional lay-out of chips – would be subject to the protection of

copyright. The American Semiconductor Chips Protection Act, however, introduced a different regime for the protection of chips which would later be adopted in Europe as well. In many countries, particularly in Asia, the absence of a properly functioning copyright system led to many cases of chips „piracy". These countries became strong competitors of the American chips manufacturers and the federal administration of the U.S.A. decided to create a form of chips protection other than via copyright. From their point of view, this approach also had the advantage that it would not have to take into account tbe generally accepted assimilation principle, i.e. equal protection for residents and non-residents of a state. Instead of this, the Americans introduced the principle of reciprocity, which means protection will only be afforded to non-residents if their homeland provides the same protection to Americans. An interim protection was granted to EEC member states until the middle of 1991, during which period these countries had the opportunity to harmonize their legislation with that of the U.S.

For some, this interim period proved that the American approach was not a protectionist one with respect to the U.S.A.'s European trade partners. This may be true, but this point of view could be argued against by the very small market share in chips of European manufacturers. More importantly, it should be stated that the colossal European market for chips was in danger of being monopolized by the above mentioned East-Asian producers. To grant an interim protection period to EEC member-states was the only way to obtain immediate protection for American producers in Europe and thus create an extra-territorial effect for the Chips Protection Act.

The interim period was in fact used by the EEC to produce a directive. On 7 November 1989, the Dutch Chips Protection Act[1] came into force. Although its arrangements are similar to those of copyright law, there are some remarkable differences. Apart from the above mentioned principle of reciprocity we would like to mention the obligation of registration (depot). For this registration an extensive amount of information about the topography of a semiconductor chip is required. It was thought that the fact that this information could be photocopied hy others has led to a very limited number of registrations in the Netherlands. While the number of depots in Germany, Japan and the United States were 112, 2870 and 5453 respectively until 1990, the number of registrations in the Netherlands up to May 1991 was only 12. In 1991 an amendment[2] to the Dutch Chips Protection Act came into force that should take away the impediments for Dutch manufacturers. Although the information required for a depot will still be public, it will no longer be allowed to photocopy it or take it away from the registration office. It will also no longer be required to state the names of the designers of the chip upon registration.

[1]Wet van 28 oktober 1987, houdende regelen inzake de bescherming van oorspronkelijke topografieen van halfgeleiderprodukten (Stb 484).

[2]Wet van 11 september 1991 (Stb. 471) tot wijziging van de Wet van 28 oktober 1987, houdende regelen inzake de bescherming van oorspronkelijke topografieen van halfgeleiderprodukten.

For large companies this has proved to be an impediment as the development of chips is usually done by a large team. The number of registered chips has, nonetheless, not drastically increased. At the end of May 1993, the total number of chips was 36.

2.2. Software protection

EEC legislators have also been rather active in the field of software protection. In April 1991 the European Parliament decided to lay down an EEC directive with respect to software protection. For Dutch law, this was not really necessary. There have been a number of cases in which the protection of software by copyright has been acknowledged. As, according to Dutch law, the prerequisite of originality can be relatively easily fulfilled, almost every computer programme in which a certain freedom of choice has played a role will be protected by the Copyright Act of 1912. Furthermore, in case law criteria have been developed for the protection of documents without the maker's own, personal stamp. This applies only to documents that are meant to be made public, and the protection is against immediate adoption from the document. As computer programmes are classified as documents, this means that practically all computer programmes, be they original or not original, are protected by copyright. There is no danger that this will lead to monopolization of the technical principles applied in these programmes. The protection of non-original documents is restricted to direct derivations. With respect to most simple programme routines it can be argued that they have been conceived hy many different programmers in many different places. They belong to the public domain.

An important reason why a European directive was laid down is the desire to harmonize the protection of software within the EEC. Strangely, this desire has not lead to a „sui generis" arrangement. On the contrary, harmonization at the European level was based on conflicting national copyright regimes. We would not plead, however, for a special legal regime for software within the EEC. A better approach would have been a further harmonization of copyright law within the EEC.

Two important differences of opinion have played a role in the debate that finally led to the present EEC-directive. Firstly, it appeared difficult to make a choice hetween the interest of the party which commissioned tlie designing of a special programme and that of the party which was commissioned to do it (in many cases a software house). This debate has been decided in favour of the commissioned party (the maker). Secondly, the admissibility of „reverse engineering" appeared to be a problem. Reverse engineering is the technique of studying and analyzing a computer programme in order to discover the intrinsic ideas and principles of a programme. Sometimes this technique involves „disassembling" or „decompilation" of the programme: the translation of the binary object code into a higher programming language, which is easier for humans to understand. It could be argued that

to disassemble the object code (or to copy it in order to do so) is not against the rules of copyright, because it does not harm the exploitation rights of the copyright holder nor does it infringe his right that the programme should not be changed. Furthermore, to forbid this technique would lead to a conflict with the principles of competition law. For according to these principles, ideas and algorithms are not protected. Nevertheless, disassembling was forbidden in the directive, although it was allowed to study a programme in order to find its inherent principles and ideas.

Where the EEC-directive seriously falls short, however, is in the status of computer interfaces. „Interface" is a rather general term, about the meaning of which even within the software industry itself there is no agreement. An interface is a connection between two entities, for example between a computer programme and a human being, or between two parts of a computer programme. An interface could be the way a set of computer files is organized by a certain generally used computer programme. If a similar computer programme – but distributed by a different software firm – would require access to the data of the original programme, the interface would have to be studied by the competing firm. Only by doing this could the later programme provide „interoperability". According to the directive, it is allowed to study a programme in order to achieve interoperability and to copy it in the course of its normal use, but it is not allowed to copy a programme or part thereof in order to disassemble it.

It is our opinion that, in the first place, copyright law is not an adequate instrument to regulate these problems. They are the province of competition law. What copyright law does, is to protect a work against undesirable changes or distribution by others than the intellectual owner. Merely to protect the „sweat" of the maker is not the task of copyright. Furthermore, the frequent use of technical terms in the directive is uncommon in copyright regulations and it will soon lead to severe problems of interpretation. The way in which the term „interoperability" is used is confusing. For example, the way in which a programme interacts with the user via the computer screen will also effect its „interoperability". However, the directive does not explain how this problem relates to the „look and feel" doctrine.

Secondly, the EEC directive is, in effect, against the interests of the European software industry. As most standards in the personal computer software market are of American origin the prohibition of reverse engineering in the directive effectively frustrates the use of these standards by European competitors.

Would reverse engineering be allowed according to Dutch law? To use de facto technical standards applied in popular computer programmes would most likely not be against Dutch competition law. To make use of somebody else's effort is in itself not illegal, unless there is a specific law or rule against it. Copying an idea or principle is allowed even if it could lead to confusion with the original product. Furthermore, in case-law[3] it has been decided that if (some of) the users of a product

[3]Klerenhangerarrest NJ 1970, 434

require a certain standardization in order to enhance the adequacy and use of the product, it would be allowed to copy certain aspects of the original product in order to fulfil the users' wishes.

However, wbether it would be allowed to copy the object code of a programme in order to study, analyze or even disassemble it, depends upon whether such copying would be considered relevant to copyright law. Technically, one could argue that the work is copied. We would argue, however, that the copy would not be an infringement of copyright law for the same reasons we gave with respect to the EEC-directive. Finally, it is not uucommon that the terms of the license agreement between a software distributor and the end user forbids reverse engineering or any activity that would lead to a similar product or part of it. In many cases, the terms of the license contract would determine the right to make use of a de facto industrial standard.

It is expected that the bill for modifying the Auteurswet of 1912 (Copyright Act) to ensure that computer programmes are protected, will pass througb the Dutch parliament in the Autumn of 1993. The bill proposes that the term „computer programme" should be added to the list of examples which are considered to be „works" in accordance with the meaning of the Act. Computer programmes will be excluded, however, from the copyright protection applicable to non-original „documents". The regulations which allow copying for private training, study or use under certain circumstances will not be applicable to computer programmes. The rightful user will be granted the right to make a copy for backup purposes. The regulation concerning reverse engineering set down in the directive has been incorporated in a separate article concerned with computer programmes. When the bill has passed through the Upper House, the protection of software in the Netherlands will be in accordance with the EEC directive, albeit rather later than the date of implementation (the first of January 1993) stipulated in the directive. With the exception of the rule on reverse engineering, this legal basis will not greatly affect the existing situation concerning the protection of software as it has developed in recent years.

2.3. Database protection

The third area in which the European Commission has undertaken legislative initiatives with regard to the legal protection of information technology is that of databanks. On the 29th of January 1992, the European Commission published a proposal for a directive which would, in the first place, provide a regime for the copyright protection of databanks. Apart from the possibility of protecting databanks as collective works in a copyright sense and the copyright protection of the (database) software, the economic importance of data itself is being increasingly recognized. It will not be often, however, that the contents of a databank will fall under the protection of copyright provisions; it is impossible to ascribe originality to data that are merely facts. Furthermore, the protection of the databank itself is

also not always obvious. This is particularly the case where the collection of data concerned is intended to be complete, hence one in which it is hard to argue that the publisher of the data has developed the databank in accordance with certain criteria for selection. This means it is not easy to show any originality. Even if there is mention of a selection process, this fact alone is not sufficient to merit copyright protection according to the Dutch courts. It is necessary that this selection should reflect the personal vision of the compiler[4].

The proposal for a directive bas chosen for the copyright protection of databases as being collective works in the sense of article 2, paragraph 5 of the Bern Convention. As far as the originality criterium is concerned, it is deemed to be sufficient if the database is the author's own intellectual creation. This distances itself from the further requirement demanded by the Dutch Supreme Court. In as far as the contents of databases are uot already protected by copyright, for example summaries of articles, the proposal introduces in article 2, paragraph 5 a sui generis protection of an anti-trust law character: „Memher States shall provide for a right for the maker of a database to prevent the unauthorized extraction or re-utilization from the database of its contents, in whole or in substantial part, for commercial purposes." In order to prevent information monopolies where the database publisher is the only source of information, the proposal provides for a system of compulsory licences. If this proposal is accepted, it is this latter regulation which will have the most far-reaching consequences on Dutch law. The present view in the Netherlands is that also data which are electronically stored fall under the category of „documents", on the basis of which under certain circumstances also non-original data files are considered to be protected from direct adoption.

3. Protection of data

A second strand in the developments of computer law is the growing tendency to protect computer data. Although the opinion seems to be growing that computer data should, first and foremost, be protected by technical and organizational measures, the interest in legal arrangements in this field has been increasing as well. This can not only be said for the developments in the Netherlands but it is also true for the international forum. In addition to the developments described above concerning the protection of data in databanks, important impetuses have been the growth in volume of trans-border data flows and the increasing interest in the privacy aspects of storage, processing and retrieval of personal data. An other important issue has been the question of whether the provisions of criminal law and criminal law procedure have been adequate in the light of what is often referred to as „computer crime".

[4]HR 4 January 1991, NJ 1991, 608, Van Dale/Romme.

3.1. Transborder data flow

By transborder data flow is meant the transport of data across national borders. It could imply sending data to or from a foreign country or the access of data from a foreign country or vice versa. For various reasons, since 1970 there has been an increasing interest in regulating these data flows. Some of these reasons are:

- The technical progress in the field of telecommunication and informatics (the combination sometimes called „telematics") makes it possible to transport data in very large quantities via many different channels. The content of these data flows cannot possibly be monitored by governments.
- Transborder personal data flow could lead to an infringement of the right to privacy. Even within their homeland it is virtually impossible for most people to know where tbere personal data are kept, whether such data are necessary and whether they are correct.
- The processing of data by one country which are vital to the interests of another country could threaten national sovereignty if the resulting information is withheld. Transport of data itself could be of interest to national security e.g. if information of strategic value is involved.
- Transborder data flow changes the balance of power between states and large firms. International companies can now make decisions that cannot be controlled by the states in which they operate. These decisions could involve matters of financial, social and political interest.
- Particularly for less developed countries, it is in their interest to keep the available data and its processing within the country itself. To export data could mean that the national hard- and software industry will not develop.

In general it can be said that data has become an economic good. This leads to the tendency by national governments to protect their interests and to regulate transborder data flows. The Dutch legislature, however, has not been particularly active in this field. Fiscal authorities generally pursue their right to information in a rigorous way, but this practice is based upon seasoned legislation. The police and the judiciary have met some obstacles, and some of tbese have been removed by the recent Computer Crime Act[5]. Furthermore, the Dutch privacy legislation[6] contains a section that regulates some international aspects.

The discussion with respect to the desirability of new legislation on transborder data flow has, so far, remained at a rather abstract level. The prevailing argument is that the regulation of transborder data flow would frustrate the „free flow of information". Some legal scholars are of the opinion that this could infringe certain constitutional rights.

[5]See below in section 3.4.
[6]See below in section 3.2.

It should be added that probably the area in which new legal rules would be most desirable, the field of international data exchange for commercial purposes („paperless trading") would require a global legal arrangement rather than one based on national or European legislation. Without such an arrangement, it seems likely that firms which operate globally will offer conflict resolution services that could replace the law.

3.2. Privacy legislation

The OECD „Guidelines for the Protection of Privacy and Transborder Flows of Personal Data" from 1980 and the „Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" by the Council of Europe which came into force in 1985 are primarily concerned with personal data. An investigation carried out by KMG Klynveld Kraayenhof & Co in 1984 into the nature and extent of transborder data flow in the Dutch business community revealed that a quarter of the transborder data flow information concerned individuals. The OECD guidelines, which are generally considered to constitute an international minimum standard for the protection of personal privacy with regard to transborder data flow, were principally designed to promote the free exchange of information between member-states. Aware of the fact that states could hinder this free exchange, because of their different approaches to privacy legislation, the OECD formulated eight basic principles which should be taken up in national legislation in order to protect personal privacy. Article 18 once again emphasises the intention behind the OECD guideline by stating that member states may not unnecessarily hinder transborder data flow in the name of privacy protection.

The treaty of the Council of Europe makes it clear in its preamble that the basic aim is to strive for a balance between the protection of personal privacy and a free exchange of information. In article 12, however, it is stated that tbe flow of personal data to other states which have signed the treaty cannot be forbidden merely to protect personal privacy if the legislation of those signatory states offers equal protection (and the data is not destined to be sent on to a non-signatory party). The treaty is based on

1. a number of basic principles regarding the material necessity for protection,
2. a prohibition on limiting transborder personal data flow if the only reason for that limitation is to protect privacy,
3. the obligation to assist foreign parties in the exercise of their rights. With regard to the latter, article 16 states that such a request for assistance may be rejected inter alia if the request is irreconcilable with the sovereignty of one of the parties to the treaty or with the rights of people in the treaty state. A strict reading of this article may, however, have an undesirable effect as the supply of data or information about automated systems will increasingly not be in the interest of the state.

The Dutch Data Protection Act[7] which came into force in 1987 also includes an international section. Article 47 declares that the Act applies to personal data files located abroad if the holder is Dutch. Personal data files located in the Netherlands, but whose bolder is based abroad, come under article 48 of the Act. Both articles contain provisions for tbe situation in which foreign legislation is applicable to the registration files concerned. Finally, article 49 is concerned with access to foreign registration files from the Netherlands to wbich Dutch law is not applicable. The user should take the necessary measures for protection and, as regards countries where there is a total lack of legislation on the protection of privacy, it may be prohibited to access the data kept in the data file from the Netherlands.

The Data Protection Act is based upon three pillars. Firstly, to make it evident to those who have been registered that they are registered, inter alia by making it obligatory to notify those concerned that they are included in a personal data file. Secondly, a framework consisting of material norms and requirements with which registrations and the acquiring and distribution of data must comply. Thirdly, to provide room for selfregulation within the various branches in the form of regulations and codes of behaviour.

The basis for the exercise of the legal rights of those who have been registered is formed by the right of inspection and the right of correction for those registered and by the supervision of the observation of the rules by the Chamber of Registration. Apart from its general supervisionary responsibility, the Chamber of Registration is also charged with judging the rules and codes of behaviour. Decisions made in this regard by the Chamber of Registration do not bind the judiciary. Those who keep and process personal data files are under an obligation to protect the data files. If someone suffers damage because the transactions have not complied with the regulations laid down in the Act for the protection of the interests of those registered, it is possible to bring an action for damages. Interested parties may bring a so-called class action. Liability also arises from a failure to adhere to the regulations or the notification requirement, providing information from the Netherlands to a personal data file located outside the Netherlands which is not subject to privacy protection agreements, or to gather data from such a data file.

In the near future, it will probably become necessary to examine the Dutch Act to check whether it is still in agreement with the proposed Council Directive (COM (92)422) concerning the protection of individuals in relation to the processing of personal data (syn 287) and the Council Directive (COM (90)314) concerning the protection of personal data and privacy in the context of public digital telecommunications networks (syn 288). These directives may be implemented in the near future.

[7] Wet Persoonsregistraties

3.3. Ownership of computer data?

A question which is often asked is whether legal provisions in which the terms „goods" or „property" appear are applicable to computer data and/or software. We support the argument that computer data and software can most certainly be designated as „goods" or „property"[8]. The acceptance of this argument would mean that new legislation in the field of informatics would not be as necessary as is often maintained.

To state that computer data and software could be classed as tangible property does not deny that most computer software and data would also be protected by copyright. In the automation industry the term software has two meanings. It can be used to refer to an intellectual product, „work" as meant by the Dutch Copyright Law[9], or as the word for a certain actual specimen of that intellectual product. The first meaning falls solely under the law of intellectual property, whereas for this discussion we would place the second meaning under tangible property.

One point of dispute among lawyers is whether computer data possesses the substantiality required of goods. To associate the criterium of substantiality with goods is considered by lawyers to be self-evident. The lack of proficiency with which terms such as software, as indeed information, are used is connected to the fact that these terms refer to concepts which are relatively new. The same was true for „electricity", and „energy" in general, at the beginning of this century. This, of course, does not mean that information and energy have not existed for a long time, but that the way in which people think about them has considerably altered.

Technological developments, and especially those of the last 200 years, mark an increasing ability to manipulate phenomena which were originally exclusively products of nature. In the first phase, spacial structures could be changed (a roof, a pot). In the second phase, objects could be made movable, manipulable (a door, the wheel). It is only in the third phase that the technical control of energy becomes possible (the steam engine, an electric motor). In the most recent phase, information processing by technical means has become possible (an automatic door, a robot controlled by a computer). The fifth phase is one that has yet to come. It would include the possibility that a computer could change its own programme and adapt it to new circumstances[10].

Increased manipulation possibilities are preceded by advances in knowledge concerning the phenomena. Initially, this knowledge remains the province of scientific researchers and technicians and it takes some time before these concepts filter through to others, for example, to lawyers. This process of the assimilation of technical knowledge is, these days, put under considerable pressure by the speed with which technical possibilities are implemented in society. This is the reason why in the early stages the discussion of the legal aspects of technological developments has a rather confused character.

In conclusion, the very fact that data can now be manipulated by technical means implies that data are tangible and could therefore be goods or tangible property. The same is true for many forms of energy, like electricity.

[8]The same is true for the term „product" which appears in the EEC directive on product liability.

[9]Auteurswet 1912

[10]When applied by humans, this skill is sometimes called „strategic planning". It is not easy, because it requires the ability to anticipate the future.

3.4. Computer crime

The Court in Arnhem[11] stated that software is goods as understood in the article concerning embezzlement and theft because „the character of the present computer data is that of transferability, reproductivity and availability, while furthermore they are economically valuable". This verdict was based on criteria from the electricity verdict[12]. The discussion that followed the Arnhem verdict has been lively. One argument was that in the electricity case the Supreme Court built in certain limitations by stating that the theft article should not be applied to „rights or intellectual products, such as, for example, copyright or a patent". We would maintain that this argument misses the point. To remove a copy of a computer program (or a computer data file, or a book) cannot possibly mean that the copyright or the intellectual product has been appropriated. After all, „intellectual product" means: the „work" in the sense of the Dutch Copyright Law, the „corpus mysticum". It is not possible unintentionally to transfer the right of intellectual property by theft.

On the 1st of March 1993, the Computer Crime Act[13] came into force. The Act contains provisions regarding criminal law and criminal law procedure. One of the key points of the Act is its focus on the individual responsibility of computer users, expressed inter alia in a security requirement as a condition for being able to bring a charge for unauthorized entry in computer systems („hacking"). The Act even extends to accountancy law with the provision that independent accountants (who are responsible for the approval of annual accounts) will be obliged to report inadequacies with respect to companies' computer security in their 'management letter'.

The proposals for the criminal law procedure would increase the police powers of search. Searches in computer systems would become as extensive as the ability of the officer to gain entry from the location of the computer terminal of the suspect.

That the Dutch Act on computer criminality has accepted the proposals made by

[11]Hof Arnhem, 27 October 1983, Computerrecht 1984/1.

[12]The Dutch Supreme Court, H.R. 23 May 1921, N.J. 564.

[13]Wet Computercriminaliteit (Computer Crime Act), Wet van 23 december 1992, Stb. '93-33 (K. 21.551).

the Committee on Computer Criminality which explicitly stated that data is not to be designated as goods under the criminal law is, in our opinion, a step backwards for the development of a clear and simple practice. The arguments put forward to justify a whole series of supplements to the law for a whole new sort of object – „data" – are hardly convincing. As a result of technological developments, it is no longer true that data are always an intellectual product. Even if they were, as soon as they took on a concrete form, they could be classed as goods as well. Data can be stolen, in the form of printed paper, in the form of a computer file on a disk, or via the telephone. Thus not only is the intellectual owner of certain data protected, but also the „everyday" owner of a book, a computer program, or a data file.

A large number of new sections is the consequence of choosing for a separate regime for data. As yet, there is nothing to indicate that it was necessary to change the criminal law code. A recent investigation commissioned by the Platform for Computer Criminality (in which participants are drawn from both business and the civil service) revealed that the most frequent offence is software piracy (47 %). This can already be dealt with perfectly adequately by copyright law. We have already argued that the criminal law code as it was already offered protection to wronged users/those who do not hold the copyright. The second category (17 %) concerns damage to data or programmes. According to the report, the damage is considered by most organisations to be too insignificant to bring an action. Only 2 % of respondents who had experienced this form of computer criminality actually pressed charges. According to the criminal code as it used to be these acts could be classified as criminal damage. The third category (14 %), consists of hacking, unauthorized entry into a protected computer system. This is probably the only offence which would not be criminal under the criminal code as it was before 1 March 1993, unless criminal damage would be involved. As far as money is concerned, by far the most important category is that of fraud and forgery, 6 %. Here, charges were pressed by 55 % of the respondents who had been the victim of such an act. The cases concerned here were probably all ones which could have been dealt with by the existing criminal law.

A separate status for data may give rise to many ambiguities in the future. Recent legal verdicts (for example, that of the Supreme Court which stated that computer files could be seen as documents for the criminal law and the verdict by the Court of The Hague in which making a computer programme inoperable could be classed as criminal damage) have shown that the existing criminal law was not inadequate. The new legislation, however, would render some of these cases obsolete.

A final argument against the new legislation in the Netherlands would be the harmonization of criminal law in Europe. The new legislation has come into force at a time in which there is no unity on this front within the EEC, particularly with respect to procedural law.

4. Conclusion

Especially in the field of computer law, it is often said that the government should initiate new legislation to deal with computer-crime, to protect privacy, to solve problems of liability, to secure copyrights etc. We strongly disagree with this opinion. It is very likely that the future would prove the new legislation to be either entirely irrelevant or even misguided. We believe that new technologies, like most other social and cultural changes, should rather put the quality of the present laws – and of present lawyers – to the test.

Legal informatics in the Netherlands

1. Administrative applications

In this article, we will not deal extensively with the administrative applications of computers in the legal field. A law office, be it a solicitor's, a judge's or a legislator's is an office like any other and the trade-offs for automation of the administrative functions are basically the same.

Although public service organizations have met severe problems due to, among other things, the lack of cost consciousness within the civil service, the lack of professional knowledge of automation and often the extremely large scale of the computer applications involved, many public services in the Netherlands have now automated their administrative processes. Examples are the tax services, the administrative management of fines in the criminal law system and census administration.

2. Automated legal data bases

The situation is different with regard to automated legal data bases, containing full texts of case law, statute law and all the other legal documentation. The trade-offs here are, of course, influenced by the total number of users (lower average costs) and the possibilities for the legal users to charge others for their costs. Established publishers in the legal field have made legal texts available in computerized form, for example, a large data base containing case law (recently distributed in the form of a compact disc (CD-ROM)) and an on-line data base with statutes and other legislation.

However, it seems to be an almost universal fact, and the Netherlands is no exception, that legal data bases are not used very often. An explanation for this could be that these systems do not provide any information that could not already be obtained equally cost effectively by traditional means. The only advantage that legal data bases have over books and magazines is that the user can ask for documents containing a certain word, or a combination of words. Apparently, this is not the kind of question lawyers normally ask.

3. Legal knowledge systems

In recent years, within the field of specialization called artificial intelligence, particularly research into the possible applications of so-called knowledge systems

has taken flight. The expectation was that here was a form of artificial intelligence with which quick results could be obtained. From within the group of knowledge-based systems, it has been the expert systems which have received the most attention up till now. The term expert system indicates that these computer programmes intend to simulate the reasoning of a human expert, with expertise knowledge in a particular specialized area. There are other features that would be required to call a programme a proper expert system. Such a programme should have the ability to learn, to communicate in natural language and to produce unexpected answers, i.e. have a certain creativity of its own.

The latter three features are certainly interesting, but will not be dealt with in this paper. We will concentrate on knowledge systems; computer programmes that are capable of containing the knowledge of one or more people (the authors of the programme) and transferring it to others, the users of the programme.

The lack of a scientific basis in law has affected legal informatics. When making a legal knowledge system, it is almost never the case that existing empirical knowledge can be used as a starting point. Extensive research (of a kind that is not familiar to most lawyers) would first be necessary before the empirical knowledge required could be obtained. What has not been put in can never be got out.

The accurate prediction of judicial decisions can be of great importance to an advocate in determining whether, in a particular case, he should agree to a settlement or bring an action. For legislators, it would be of interest to be able to predict the expected social effect of a piece of draft legislation. These are examples of the pragmatics of the law, of how the law works.

We do not know very much about the syntax and the semantics either. For example, we do not bave useful theories about the word usage in legal texts and we do not know much about the meaning of words and sentences. We have no theory which could help to derive from the written verdict of a case which legal subject the case deals with, or what the verdict was. Therefore it is as yet impossible to use a normal, full text legal data base as a direct support to a knowledge system.

Another example of the importance the use of empirical research could have in the construction of a legal knowledge system is the following. In an advice system which offers help in making decisions concerning whether or not to remand in custody, problems arise regarding the specification of terms like „danger of abscondence" or „danger of repetition". A knowledge system cannot, at present, do much more than ask the user whether he considers this danger of abscondence or repetition to be present and to give some explanation concerning the current notions of what these terms mean on the basis of case law. This situation could be improved if more empirical research on these subjects was carried out.

4. Computer advice systems

As empirical knowledge of judicial matters is so limited, it can be concluded that the construction of a legal knowledge system is, at this moment, impossible. With

this limitation in mind, research was undertaken by the Worksbop for Computer Science and Law at Erasmus University as to alternative means for supporting lawyers' work with the aid of a computer. From that research, it has appeared that there is a substantial role for the computer to play if sufficient attention is paid to the interaction between system and user. What we are referring to here is not a knowledge system or an expert system but a computer advice system; a computer programme that is able to advise users about a specific legal subject on the basis of day to day legal proficiency. An important starting point for this sort of system is that it is a means for legal authors to convey their own opinions to the users. The term „opinion" is used deliberately. This is to emphasize the difference between empirical knowledge (that can be tested and falsified) and the kind of practical knowledge lawyers have, that cannot be tested and falsified[14].

5. Could computers replace judges?

If – in the distant future – legal knowledge systems or even legal expert system would become a feasible proposition, could they possibly replace judges?

As our brief outline of technological developments has shown[15], computers are not yet capable of changing their own programmes in accordance with new developments. People are not always capable of doing this either, but they are far better at it than computers. In law, and especially in judicial decision making, the question at stake is: is the rule still applicable?

Scientific theories (and, in particular, tbe fractal theory), have shown us that it is hard and sometimes even totally impossible to predict the future with anything like accuracy. Yet computers that are designed to make legal decisions would have to be programmed for the future. People, on the other hand, can perceive and assess changes in the environment. Finally, it should be mentioned that even if a machine could make sensible legal decisions, only humans could be held accountable for any such decision.

6. The danger of „fourth generation legislation".

After spoken law, written law and printed law, we are now ready for fourth generation legislation: law by computer. The law would take on the form of a computer programme. This programme would put questions to the judge (or administrator, or citizens) and the programme would then state the obligations and the rights of the parties involved. It could do this in a detailed way and in accordance with how the legislator wanted the rights and obligations to be at the time of drafting. The judge would be „la bouche de la loi" again, and this would set us back to just after the French revolution.

[14] A number of these computer advice systems have been made at Erasmus University as a part of the JURICAS project. They are distributed by Royal Vermande Publishing Company, Lelystad, the Netherlands.

[15] Section 3.3

Unfortunately, given the incentives of legislators and civil servants, as well as politicians, it is very likely that this form of legislation will soon be introduced. It would mean that the role of the judiciary would be reduced in favour of the legislative power. It would therefore render the law more inflexible then it is at present. The alternative is that there should be less, and less detailed, legislation in the first place. Our society will need human judges to interpret the law for future situations.

7. The „technology push" towards centralization

In order to steer the behaviour of people in an organization, relevant information must reach the administrator in time so that he can make a decision at the proper moment and, in turn, that decision must be communicated to the person to be steered in time. This is often physically impossible and the organisation is forced to assume a decentralized structure – or go under.

This example from management science shows that information exchange is costly. Coase, as an important business science theoretician, has distinguished between general (or scientific) knowledge, which by virtue of its universality and objectivity can easily, and therefore cheaply, be conveyed and specific knowledge (or information) which, possibly because of the demands of timeliness, can only he conveyed with difficulty and the incursion of high costs. Examples are quickly fluctuating prices of goods in a certain decentralized area; information about the sudden behaviour of competitors; specific opinions of certain clients, etc. If the availability of such specific information is of great importance to the realization of the aims of an organization, this will also lead to decentralization.

Decentralization leads, in turn, to costs; the administrator must then supervise those carrying out the tasks and make sure that they are not striving for the wrong aims, etc. These costs are often referred to as agency costs. The level of decentralization of an organization depends, therefore, on a trade off of both sorts of costs: information costs and agency costs.

In a time of automation, it is not surprising that the administrators of organizations try to facilitate and speed up the information exchange by using computers and computer networks. Unfortunately, these means are not without cost either. They could change, however, the trade off between agency costs and information costs in favour of more centralization. This is true both for companies and for state organizations. Fourth generation legislation is only one example of this growing tendency towards a higher level of centralization.

Conclusion

In this article, we have discussed the relationship between information technology and law in the Netherlands. The first aspect that was considered, that of computer law, examined some of the matters that have caught the attention of the legislating authorities in the Netherlands. The second aspect, that of legal informatics, showed that there is an increasing tendency to apply information technology to the Dutch legal system. The common denominator of both aspects is the fact that electronic data and information flows have become an important economic and social factor. It is, therefore, only natural that those who work for state organizations will try to maintain and where possible expand their control of information flows.

The EEC has had a considerable influence on the development of Dutch law with respect to information technology. The activities by the EEC to harmonize the legal rules in this field have not always been optimal from the Dutch point of view, and sometimes not even from the European point of view.

As regards the use of information technology within the Dutch legal system, the EEC has hardly exerted any influence. We would suggest that an EEC directive against fourth generation legislation in member-states could prevent a tendency towards centralization and the increasing inflexibility of the law at the national level. *

* * *

SUMMARY

Centrum pro počítače a právo na Erasmově universitě v Rotterdamu

Autoři se v tomto článku zabývají dvěma základními problémovými situacemi, které vznikají ve spojení práva s počítačovými technologiemi. První z nich vzniká ze skutečnosti, že užití počítačových technologií působí obtíže, které zákonodárce nepředpokládal, druhá ze skutečnosti, že užití těchto technologií jako nástroje právníků mění jednak způsob, jakým pracují, jednak samu jejich profesi.

V první části příspěvku se autoři zaměřují na dopad prudkého nárůstu významu informačních technologií na právní řád, a to jak nizozemský, tak evropský, poukazujíce především na nepříznivé důsledky kopírování amerického přístupu k ochraně informačních technologií, zejména čipů, databází a software obecně, v harmonizačních směrnicích Evropských společenství. Autoři se v této souvislosti obsáhleji věnují především otázce legality reversního inženýrství, nezbytného pro další rozvoj evropského softwarového průmyslu s ohledem na skutečnost, že většina základních programových postupů pochází z oblastí mimoevropských, přesto však směrnicí z ro-

*This article is a revised version of an article that appeared in the European Review of Public Law, vol. 3, no. 1, Summer 1991 („Computers and law in the Netherlands").

ku 1991 takovou činnost zakazuje.

V oblasti databází se autoři zabývají v prvé řadě harmonizační tendencí, projevující se v návrhu směrnice Komise ES z ledna 1992, která směřuje k autorskoprávní ochraně databází jako kolektivních děl.

V souvislosti s ochranou dat je v příspěvku zdůrazněn zejména význam, který evropské země přikládají mezistátním tokům dat a ochraně osobních údajů při jejich zpracování počítačovými technologiemi. Zdůrazněna je skutečnost, že data musejí být, jsouc manipulovatelná technickými prostředky, považována za věci hmotné a jako taková mohou být hmotným majetkem, podobně jako jiné formy energie, například elektřina.

Skutečnost, že data je nutno považovat za zboží byla konstatována i v nizozemské judikatuře (rozsudek soudu v Arnhemu z 27. října 1983). Navzdory tomu byla v novele nizozemského trestního zákona z roku 1993 data pojata jako specifická kategorie od ostatního zboží se lišící, což způsobilo nutnost komplikovaného a neopodstatněného doplňování stávajícího předpisu.

Přitom je téměř polovina trestných činů v oblasti informačních technologií řazena do kategorie počítačového pirátství, tedy snadno postižitelná zákony na ochranu autorského práva, a i další rozsáhlé kategorie počítačových trestných činů spadají do již známých trestněprávních skutkových podstat, snad až na nedovolený vstup do informačních systémů.

Pokud se právní informatiky týče, autoři konstatují hojné používání počítačových technologií v administrativě, ovšem velmi nízké využívání systémů zpracování dat v běžné právnické praxi (jedinou výhodou právnických databázových systémů je podle autorů vyhledávání podle slov či klíčových úseků, což však není zcela běžným způsobem právnického získávání informací), kde jsou klasické tištěné informační zdroje srovnatelně více cost effective. Vytváření systémů, které by byly schopny řešit konkrétní právní otázky, brání především nedostatek empirického poznání v oboru a pevné vědecké báze práva, proto se i autoři ve výzkumných programech Erasmovy university zaměřili spíše na užití počítačových technologií ve vytváření systémů schopných poskytnout up-to-date informace a moderní prostředky vědecké komunikace.

Konečně ve zvláštní pasáži se autoři věnují otázce computerizované legislativy, tzv. legislativy IV. generace, která podle jejich mínění opět snižuje soudce na úroveň sluhy zákonů a v otrockém pojetí vrhá vývoj práva zpět.