

Summary

Chapter 1 Introduction and research subject

The onset of the ‘information age’ has led to a boom in legislation in the Netherlands, the European Union and beyond. New technology seems automatically to generate new laws.

The question posed in this study is whether information technology, and the social developments associated with information technology, really makes new laws necessary.

In the first chapter of this study attention is paid to the relationship between technology, social developments and the role of the law. Two starting points are made explicit:

1. Social developments arise from, or are at least influenced by, technological developments; and
2. Human behaviour is explained in terms of maximising utility, in other words, people make decisions based on what will yield the most utility for themselves (the rational model of man called the REMM: Resourceful, Evaluative, Maximizing Model – JENSEN & MECKLING 1994).

For a full understanding of the first starting point, it must be pointed out that technology influences social developments both directly and indirectly. For example, a direct effect of the invention of the combustion engine was its application to cars. The indirect effect of this technological innovation was the creation of commuter suburbs. Furthermore, the influence of tech-

nology is often cumulative. Social developments may have been preceded by more than one technological innovation.

Technological development is not a spontaneous process. Four factors are needed to bring about technological development: creativity, a rational society, experimentation and mathematics.

In addition, social developments are also influenced by processes in nature, to which independent meaning must be subscribed, for example, evolution and radical natural phenomena.

The way in which a law is expected to work will be influenced, if often implicitly, by which model of man is used to describe, explain, predict and influence human behaviour.

It can make a considerable difference whether the basic premise is that laws have a decisive effect on people's behaviour or whether people see laws as only one aspect that will be taken into account in their decision-making. In the first premise, drawing up rules will be sufficient to alter people's behaviour. In the second premise, it would be necessary to study how the rules work in relation to other factors that could determine an individual's utility considerations.

The REMM rational decision model predicts that technological innovations will be applied if they are useful to someone, in a way which achieves the most utility for that person. Forbidding the certain use of a technological innovation does not in itself guarantee that it will not be used. What it does affect is a person's utility considerations. This produces a new situation, which again will be considered, and a decision will be made based on the modified utility considerations.

In this study, the term 'law' will be understood to mean 'demands and authorisations issuing from state organisations'. Apart from the function of conflict resolution, law is also considered to have a norm function: it determines those norms dominant in society. In addition, it may be said to have a facilitating function giving form to interactions.

Based on the starting points, two 'conclusions' can be drawn:

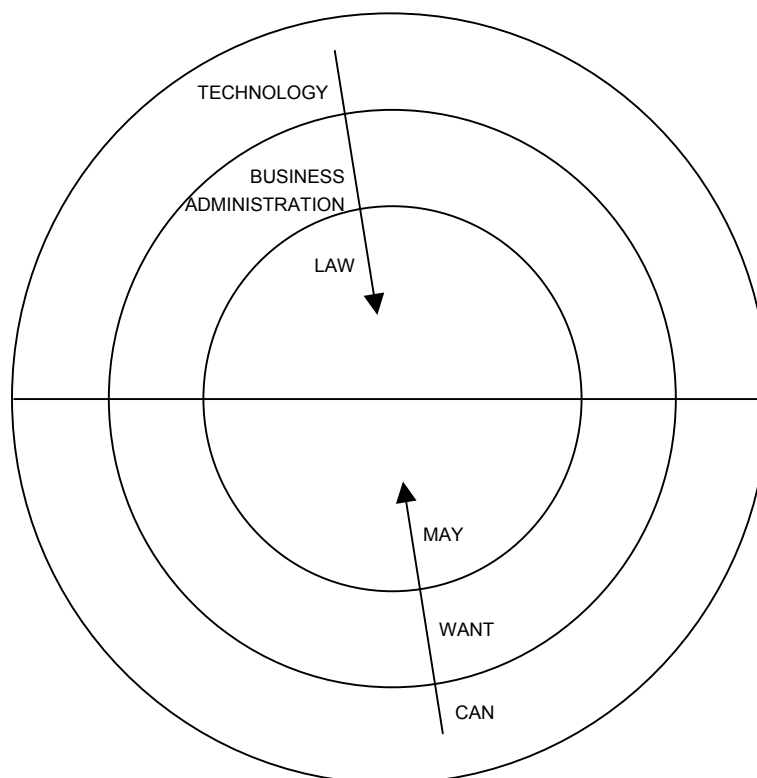
1. Since the law is intended to normalise and facilitate social changes, and social changes are connected to technological developments, effective legal measures require insight into the dynamics of technology. And that insight requires at least a basic understanding of technology.

For example, if technical measures to prevent illicit copying do not work, then legal protection for those technical measures will be equally ineffectual.

2. In order to achieve a meaningful discussion concerning the utility of new laws, it is necessary to make explicit the model of man that forms the basis of statements made concerning those laws.

For example, if the popularity of coping at home via the Internet is explained in terms of cost effectiveness, then legal measures to promote the use of digital rights management will be rather pointless.

The consecutive dependence relationships between technology, social developments and the law are represented in a model.



CONCEPTUAL MODEL FOR INTEGRATED LEGAL SCIENCE

The model consists of three concentric circles.

The outer circle encircles 'Can', the Technology. The basis for this model is positivism, in other words that one reality exists and that that reality can be known.

The middle circle covers that which people 'Want', within the limits of what is possible, using the REMM as the model for explaining human behaviour. As a multidisciplinary science, business administration offers a structure to obtain insight into (individual) utility considerations.

Finally, the inner circle is the domain of the law, of 'May' (and 'must') of demands and authorisations, of norms and facilitation. Law is an artefact for the facilitating of human interactions, for example in the form of 'property', 'majority', 'marriage', 'purchase', and through fixing norms and sanctions it delineates the external boundaries of human 'Want'. The law can steer 'Want', but is not decisive, and is itself limited by Can.

Chapter 2 The Internet

In the second chapter, further attention is paid to the Internet as an application area. A distinction is made between legal questions regarding how digital technology fits into the law and legal questions that arise from the practical application of information technology.

The former type of question may be considered as 'pre-questions'. They concern questions on the qualification of digital technology; whether digital technology makes it necessary to implement a 'digital regime' in the law in addition to the traditional 'paper regime'. Of particular significance here is the definition in property law of electronic data files, the copyright status of data processing (the temporary technical copy) and the evidential status of electronic data files.

With respect to those legal questions, which arise from the practical application of information technology, the answers to the 'pre-questions' are in the first place of importance. Only then does the question have to be posed whether the applications stimulate new social developments which need the application of new rules. This study focuses in particular on 'home copying' via the Internet, sales via the Internet, privacy and computer crime.

In order to judge the rationality of the various laws, it is useful to distinguish which aspect of the technology is addressed by the regulations.

1. Information technology itself may be the subject of legal regulation, for example the legal protection of information products,
2. The legal regulations may be concerned with the implementation of information technology, for example producing a legal framework for 'electronic signatures', or

3. The legal regulations may regulate the social consequences of the application of information technology, for example in the areas of privacy and criminality.

Chapter 3 Characteristics of the information age

As the 'information society' plays an important role in the process of new legislation – for example, the EU directives speak of the 'services of the information society' – Chapter 3 examines the information age.

In order to describe and explain the information age using an objectively definable characteristic, a connection is looked for with the stages of development of technology (VERHOEFF 1980, p. 247; DE MULDER 1984, p. 95).

1. The first stage is characterised by the ability to influence spatial structures, for example building a hut or a house.
2. The second stage consists of the possibilities for changing spatial structures, for example the wheel or hinged doors.
3. The third stage gives the possibility to control the powers that are necessary to bring things into motion. The invention of the steam engine announces the age of the industrial revolution.
4. The fourth stage offers the possibility of using the energy stored in an artefact to allow the artefact to start or stop itself etc.

The information age can be associated with the fourth stage in the development of technology. It is characterised by the ability of machines now also to process information, something that formerly only people (and animals) could do. The computer is to information processing what the steam engine was to the use of energy in artefacts. For this reason, this age is referred to as the 'second industrial revolution' or the 'information revolution'.

'Data' is a general term used to indicate all possible patterns that may contain information. It includes, for example, ink spots, rows of ink spots, words, pictures, spoken or written numbers, patterns in electro-magnetic waves, on magnetic tapes or disks etc. (DE MULDER 1984, p 23).

The development of the Internet can be connected to the cost of the various functions of computers. Per unit (kilobyte) the costs of the processing of data are the lowest, followed by the cost of storing data. The cost of telecommunication – the transfer of data – has always been the highest (MENDELSON 1988). The compression of files, higher data transmission speeds

and lower tariffs for telecommunication have increased the cost efficiency of exchanges of data via the Internet.

With respect to the control of digital data, it was concluded that the possibility to manipulate electronic data files is inherent in the application of digital technology.

Chapter 4 Why does the Internet give rise to legal questions?

In chapter 4, it is explained that legal questions regarding the Internet are connected to technology – in particular the increased accessibility of data as a result of digital technology – and the decreased cost. However, this does not have to lead to *new* legal questions.

As the Internet can best be considered as a collection of communication protocols rather than as an autonomous, physical network, it is concluded that it is not possible to speak of ‘the Internet’ as an object that can be regulated.

With respect to the characterisation of the Internet as a virtual network, the following conclusion arises:

The Internet is not a ‘new’ world, separate from the existing world. The Internet as a ‘virtual world’ is a metaphor. Behaviour exhibited on the Internet may sometimes avoid the application of rules, but not the applicability of those rules. All existing legal rules are also valid for the Internet.

The Internet may then not be a real object for regulation, but nonetheless it gives rise to two questions that are related to the communication function of the Internet:

1. the controllability of electronic data files and
2. the reliability of telecommunication.

These questions really belong to the area of information security and have a more factual character than a legal character. The solution for these problems is then to be found in the use of cryptographic techniques. The encryption of data files makes it possible to send electronic files freely over the Internet without them being accessible to unauthorised persons. With respect to cryptographic techniques, special attention is paid to:

1. single pad encryption, as this form of code cannot be broken;

2. asymmetric encryption, because this form of encryption answers all the problems with respect to telecommunication (the identity of the sender, the authenticity of the message and, if necessary, the confidentiality);
3. steganography, as this technique makes it impossible for third parties to realize that the file contains a message.

It can be remarked that the power of encryption is partly determined by the intention of the participants to the communication to keep the data confidential. In situations where that is not the case, for example home copying via the Internet where the participants actually want to make the data passed between them accessible, the expectation is that the use of technological measures will not be successful.

Chapter 5 The 'digital regime'

The first legal question is whether information technology gives rise to the need to implement a 'digital regime' in the law. This has been said to be necessary because the present system of law is too geared up to conceptualising a 'paper regime'. Whether a 'digital regime' is desirable depends upon how the law qualifies digital, electronic data. This 'pre-question' is dealt with in chapters 6, 7 and 8 in the sub questions of whether data are 'goods', whether data processing is 'reproduction' and whether data can be used as evidence.

The discussion concerning whether data have the status of property, in particular whether data are goods in the private law sense or in the criminal law sense, has been troubled by a number of arguments that appear not to be relevant to answering the question at issue. These arguments are then dealt with separately in chapter 5.

The most important argument is that data 'as such' form a special category. The question whether data are tangible objects is often answered in the negative, the reason given being that data 'as such' cannot be tangible. In the jurisprudence explanations are seldom given of what is meant by data 'as such', and an explanation is never given of the difference between 'data' and data 'as such'. It would appear that by data 'as such' is understood data that are abstracted from the carrier on which or in which they are embodied, so that the statement if examined more carefully says little more than that 'abstract' is not 'concrete'. However, the question is what are data if we do not abstract, but concern ourselves with the concrete patterns. Once abstracted, cars 'as such' are similarly not tangible objects, whereas no-one disputes that cars are the subject of property law.

That data are intellectual products, and that the copyright regime is therefore already applicable, that data are multiple, and that data cannot be

appropriated, are all arguments which do not hold up on closer examination to determine whether data have the legal status of goods. In part the discussion seems to be based on semantic differences. Once these differences are set aside, and the term 'data' is avoided, the issue is really whether the patterns (ink spots, ink spot rows, words, pictures, spoken or written numbers, patterns in electro-magnetic waves, on magnetic files or disks etc) are physical objects or not. The possibility, however, that the same confusion may arise regarding the distinction between the patterns and the interpretation of the patterns cannot be excluded.

One argument that is not based on the alleged intangibility of data is that the ownership of data (which is possible if data are 'goods') is undesirable from the point of view of freedom of information, although this undesirability seems to arise from the perception of data as having a multiple character. Quite apart from the question of validity, this argument can be rejected for two reasons. The first reason is that the civil law concept of property of (certain) data is far less extensive than the intellectual 'property' of (similar) data, whereas the intellectual rights regime is, in practice, constantly weighed against the importance of freedom of information. This can be seen, for example, in the exceptions that have been built into the law of copyright in order to take freedom of information into account. The second reason is that exceptions, if necessary, may also be made applicable to property in civil law.

Chapter 6 The proprietary status of data

To determine if data are 'goods' depends upon whether data are tangible objects, whether they are capable of being controlled by people and whether they are objects with an economic value. Although it is conceivable that there are tangible objects that cannot be controlled by people, vice versa is not so likely: that there are things controllable by humans, which are not tangible. The fact that data can be controlled by humans, and they can be produced, processed, stored and transferred indicates in itself that data are tangible objects and of value to people.

Data are not rights but nonetheless they can be the object of rights. Data do not belong to the world of ideas.

With respect to whether data are tangible objects, it appears that insights from physics play a role, although not always a decisive one. In general, there appears to be three schools of thought:

1. data are intangible and therefore not goods;
2. data may well be intangible but in practice they are always connected to a carrier which is tangible;

3. if physics does not consider data to be tangible, then tangible has to be interpreted in legal terms.

The question is very relevant, particularly because of electronic data processing. In the case of magnetised plastic disks, the magnetic fields are sometimes categorised as physical and sometimes not.

Otherwise than is suggested above, that the legal status of digital, electronic data determines the desirability of a 'digital regime', it seems that the desirability of a 'digital regime' is decisive for the legal status of digital, electronic data.

The idea that the tangibility criterion based on physics should stand in the way of categorising data as 'goods', cannot be supported by insights from physics. Experience points rather to the opposite conclusion: that as our knowledge of nature grows, more and more natural phenomena can be controlled by humans. Technology plays an important role in this respect. The tangibility of matter is not disputed. That gasses could be goods was hardly conceivable in the time of the Romans, but when gasses could be stored in bottles ideas changed. Energy became a legal object when energy became transferable, it could be accumulated and made available. Just as the increased controllability of energy characterises the third stage of technological development, the fourth stage of development is characterised by the increasing controllability of data.

Opting for a 'digital regime' could be explained in that other legal consequences would be desirable. However, that does not appear to be the case. Within the realm of private law, data files are sold and delivered, whereas the criminal law takes action against the illegal copying of another's data. The legal consequences connected to the status of 'good' also appear to be equally desirable for data.

Chapter 7 The copyright status of the temporary copy

The following question concerns the legal status of the 'temporary copy'. Starting up a computer program, looking at a text, listening to music and surfing on the Internet, in a digital, electronic environment all take place by transferring data between the various components. This process is sometimes referred to as 'copying'. Where works protected by copyright are concerned, copying (reproduction) may only be carried out by the copyright holder. It is therefore presumed that all the actions referred to above are dependent upon the permission of the copyright holder.

To apply the copyright concept of reproduction to the internal transfer of data in machines would seem to be a particularly mechanistic application of a mechanistic interpretation. In the first place, there is no reproduction in the sense that independent copies exist which can be used independently or be transmitted. In the second place, the actions of the user (in the information age, we are not 'readers' anymore, or 'listeners' or 'spectators', but 'users') are not intended to create additional copies, as the reproduction is merely secondary to enable the user to read, listen or watch.

Neither do there seem to be good grounds for bringing the internal data processing under the legal concept of reproduction. There is an exception in copyright law for the 'legitimate user'. For this category of user nothing changes. Apart from the question of when is someone not a legitimate user, and apart from the problem of enforcing a law of such considerable scope, the measure comes down to a prohibition on reading, listening or watching. It is improbable that a judge would forbid the reading of a text solely on the ground that the reader thereby infringes the duplication right of the copyright holder. This does not alter that, for example, the copying of a text in order to take the copy home and read it there may be an infringement of copyright, or that there are other conceivable circumstances in which the reading or viewing of information would be an infringement. However, this does not mean that it is necessary to classify the temporary, technical copy as duplication.

Implementing a computer program in the working memory of a server, which makes it available on various terminals, (or going along all the computers in the morning with one floppy) is already wrongful as infringing the copyright holder's right to make it available to the public (the argument was advanced at the time of the EU directive on software protection).

Finally, as computer users already copy, even when they know or suspect that this is unlawful, it would seem rather pointless to expect that this behaviour can be further limited by additional legal means.

It could be argued that this illustrates the phase of assimilation of the new technology. In the fourth stage of development of technology, machines can interpret data, something that once only people (and animals) could do. As it is exactly this function that the law attempts to limit, we see that the unlawfulness of certain (human) behaviour is now being attributed to machines.

Chapter 8 The evidential status of data files

The third question, which could point to the desirability of a 'digital regime', is whether electronic data files will be admitted as evidence. The first question would be whether electronic data files can be categorised as 'writing' and whether they can be 'signed'. The second question is what the evidential value of data files is.

The definition of 'writing' which is often found (in Dutch jurisprudence) is 'a carrier of understandable characters, which render a thought'. This definition is not a suitable one for a number of reasons. That an element of the definition should be 'a thought', is an unnecessary limitation on the concept of 'writing'. It would exclude the results of data processing or the results of measurements carried out automatically, and that is not the case. The word 'understandable' is part of the concept 'characters'. Finally, the importance of having something in writing is not the carrier, but the data it contains. This is even more the case in a computerised environment where it is quite simple to move data from one carrier to another. A definition which would take this into account would be:

A written document is a data file that contains characters.

With respect to the signing of a written document, this is in practice not restricted to 'a hand-written signature of the signatory'. For example, signatures on faxes and printed signatures have been given legal force. Furthermore, 'a hand-written signature of the signatory' is in itself not always decisive, given the possibility for manipulation by means of information technology. What is important here is a sign from someone which is suitable to authenticate the document and show that it is genuine.

A signature is a means for awarding an evidential value to a written document by or on behalf of the one who is thereby identified.

Whether electronic data files can have evidential value depends upon the reliability of the files themselves rather than on their legal status. Asymmetric encryption is a suitable means for this. The authenticity of the written document can be determined in the encrypted form.

This makes the legal framework of 'electronic signatures' pointless. 'Electronic signatures' are used because they are useful. That asymmetric encryption satisfies legal requirements is not because of legal regulation, but because of the reliability of the technology. In other words, there can only be a law on 'electronic signatures' because it comes within the outer

circle 'can' (see diagram), and therefore the law is not necessary. However, the condition that 'electronic signatures' must be based upon certification by a third party represents a step backwards because it has a negative impact on individual utility considerations. It is usually not in the interests of companies to outsource the automated data processing with respect to security.

The examination of the issues dealt with in chapters 6 to 8 has not given grounds to argue that information technology makes a 'digital regime' necessary.

That electronic data files can be 'goods' would seem to be the obvious consequence of the fact that they can be processed, stored and transmitted.

That data processing, the internal exchange of data between the different components of a machine, does not have to be of significance to the law would seem to be the obvious consequence of the fact that law does not deal with the 'behaviour' of machines.

That certain electronic data files may satisfy legal requirements would seem to be the obvious consequence of the reliability of the technology used.

Chapter 9 Legal developments

Chapter 9 reviews a number of legal initiatives concerned with the application of information technology. It then appears that the new laws to a certain extent do connect to the introduction of a 'digital regime'.

In the area of intellectual rights, we can see for example that the prohibition on the reverse engineering of computer programs is based on the idea that a temporary copy is an infringement of the copyright holder's right of reproduction. This idea has spread to database law and Internet copyright law. As a consequence, many of the stipulations were necessary to regulate exceptions and law enforcement, such as the protection of technological measures, and such stipulations show little insight.

The exchange of electronic files in order to enter into contracts, is seized upon in order to create a specialised section in the law of commerce, under the name 'Electronic property transactions'. This includes the regulation of 'electronic signatures' and the 'information society services', in particular the on-line *sale* of goods. Categorising a 'sale' as a 'service' is a legal aphorism, yet the only basis for this is the fact that the communication takes places electronically. However, there are other considerations for arguing that the regulations are irrelevant. Giving purchasers information is already embedded in a rational way of conducting business. After all, a rational

purchaser will not readily enter into a contract without having certain information. Finally, it is not likely that these obligations will provide purchasers with protection against those who offer goods in bad faith. Rather the unscrupulous seller will profit from the appearance of reliability these obligations create.

Unnecessary regulations can also be seen in the areas of privacy law and what is commonly referred to as computer crime. They are superfluous on the one hand because technology can often achieve a better result than legal regulation, for example with respect to cookies and spam. Protection against cookies and spam, as well as against viruses and spyware, can be provided by all sorts of technical facilities, which are now often standard on pc's and offered by Internet providers. On the other hand, technology may make it impossible for the aims of the legal regulation to be realised, for example in the area of encryption. As described above, non-breakable encryption is a reality. Furthermore, encryption can be successful disguised so that third parties are not aware that the message is encrypted. Finally, if the exchange of messages takes place via public news groups, there are even no traffic data, which means that even the existence of the contact is not evident to third parties.

In particular in the Netherlands, a substantial number of new regulations with respect to computer crime have emerged as a consequence of the 'vision' that computer data do not fall under the goods regime, but require a special form of treatment. This 'speciality' would appear not to find expression in a regime in which the legal consequences deviate from those of the goods regime, but remarkably in a regime that aims at exactly the same legal consequences.

The position of Internet providers appears to be 'special' in the sense that, as intermediate service providers, they are held responsible (by varying and sometimes conflicting sides) or made responsible for the behaviour of Internet users. The results seem to be less special: Internet providers can establish themselves just like 'ordinary' enterprises, they are not liable for any wrongful or illegal behaviour by their clients and they are also subject to the law. It is also nothing special that they must provide information when lawfully requested to do so, or that in certain cases information must be supplied to private individuals. Some of the obligations, however, in particular the tapping of networks, the extensive period of storage of traffic data and cooperation with respect to the decrypting of encrypted communications, cannot be expected to achieve much.

Chapter 10 Final considerations

The conclusion reached in this study is that information technology, and the social developments arising from it, does not require the new laws that were examined in this study.

The information age does not necessitate the implementation of a 'digital regime' in the law, just as the industrial revolution did not necessitate the introduction of an 'energy regime'.

Furthermore, it would appear that many legal developments, put forward as the consequence of social developments in the information age, have no practical significance.

Just as was the case with energy, it appears that the new laws on data are particularly necessary with respect to the infrastructure for data communication, such as lay out, management, maintenance and distribution, access and protection.

The social developments in the information age are connected, to an important extent, to mobility and globalisation and the problems associated with that: migration, clash of cultures and safety issues. These issues increasingly demand an international approach.

That laws are not necessary is based on various grounds:

- *Laws are equally applicable to the Internet*
Under the motto 'what is applicable off-line must be applicable on-line' a new on-line regime was created that is totally unnecessary, because what applies off-line also applies on-line.
- *Laws have open norms*
Under the premise of creating 'technology independent law', a new regime based on information technology is being created. This is not necessary, as many laws appear to be technology independent already.
- *The protection of technology is regulated already*
Chips, software and databanks might be new products resulting from information technology, but they are not new in the sense that they would fall outside the existing framework for intellectual rights. That the protection may not always be effective is inherent in the digital technique, and this cannot be counteracted by more legal protection.
- *The introduction of technology would take place anyway without the direction of the authorities and without serious consequences*
'Digital signatures', for example, were in use before the EU directive. It is not likely that the Directive will influence the increasing use of digital signatures.

- *New social developments as the result of the application of information technology are still hardly evident*

It is a point of discussion whether a development is 'new' or not. However, it would appear that the flexibility of labour, for example, is a more obvious new development than, for example, home copying. First it was the car that led to workers moving from the place of work out into the suburbs. Now it is conceivable that the influence of information technology on the organisation of labour will lead to the place of work moving with the worker and that work will be conducted in differing forms of working relationships. Just as in the time of industrialisation, it is possible that there will be consequences for labour legislation and social security. (At the same time, however, it can be said that through the impetus of the industrial revolution, much regulation has taken place already.) Home copying, as a product of the information age, may be threatening for the commercial music industry and other information producers, but it is no more than that. It would be different if home copying would, for example, lead to a permanent check on the origin of information to citizens. What we do see is that the authorities seize upon the new technology for the so-called anticipating criminal investigation. It is too soon to draw conclusions, but ideas on privacy seem to be influenced by information technology, although it is the case that safety issues and the threat of terrorism contribute to this.

- *It is not at all easy to regulate technology to keep an eye on undesirable consequences*

If home copying, on a scale made possible by the Internet, would be seen as undesirable, then it would seem that the copyright harmonisation directive can do very little more than what can already be achieved by existing copyright laws. And these existing copyright laws are having less and less affect. Furthermore, the reliability of business partners, for example, is not a matter that can be 'regulated out of the way' by 'electronic signatures' and documentary formalities. Similarly, the reliability of administrations and other electronic files cannot be compelled by law.

- *Norms remain valid in a society that is changing under the influence of information technology*

It is remarkable that as information becomes more accessible, the attempt to block access to information becomes more marked. The limited accessibility of information in an analogue environment was not the product of a legal attitude to norms, but it arose from the technical circumstances (and costs). Now that the digitalisation of information has changed the position, it should not be presumed that the former impossibility of accessing information was a normative choice. Although it is

accepted that legal regulation was not necessary as the technology was not in place to make home copying possible, that does not automatically mean that something that was not at first possible, but is now, should not be allowed. Similarly, that information that used to be accessible but is not any more does not automatically mean that there is a right to information, based on compulsory licences.

The conclusion was, therefore, reached in chapter 10 that computer law is more a matter of interpreting and applying existing laws than developing new laws.

If new laws cannot produce a different effect than the old laws, then it is simply a waste of money to make these new laws. In this study, these unnecessary laws are referred to as ‘phantom legislation’.

The term ‘phantom legislation’ covers laws that apparently regulate something as well as laws that regulate something apparent.

Examples of the first one – situations where information technology does not require legislation because they are already covered by existing law – are the numerous directives in the field of intellectual property and the legal framework for ‘electronic signatures’. Examples of the latter – situations where information technology makes legislation obsolete – are the regulations concerning cookies and spam, and the obligations laid upon network providers to cooperate with official authorities in tapping and decrypting encrypted messages.

The model is a means to prevent the devising, proposing, implementing, approving etc of useless laws.

The model shows that sometimes technology can be used to do something which the law cannot restrain, and sometimes that technology makes something possible that does not have to be restrained by law. It is also apparent that sometimes something comes into existence without the necessity of legal regulations and that sometimes something does not come into existence, even though there is legal regulation. The model offers assistance in evaluating whether something is as it is because of technology, or because that is what people want or because of a legal norm.

From the perspective of business administration, the model would seem to indicate limiting the authorities to their more traditional tasks.

The conclusion that IT legislation is not necessary is somewhat unsatisfactory given that so many IT laws have been passed. In chapter 10, various explanations for this were considered.

The most important explanations seem to be the industrial lobby and retention of the powers of the authorities. However, if the conclusion is that the new laws do not improve upon the previous situation, nor motivate social change or changes in behaviour, then these new laws must be evidence of a non-rational approach to information technology. In those cases, a decision could have been made, for example, to ignore the industry lobby.

This would appear to contradict the fundamentals of the rational decision model of the REMM, which is integral to this study. This is, however, not the case. Public choice theory explains that making laws, even laws that are not rational, is rational for lawmakers. Treating technology in a more rational way would lead to less laws being made. It would not lead to other laws that are necessary, because it appears that they are not necessary. Making fewer laws is not rational for lawmakers.

Now it is clear that lawmakers will not themselves choose to make fewer laws, one obvious recommendation would seem to be the structural under-financing of legislative departments. Then if money is going to be wasted on unnecessary laws, it will at least be not so much money.

The legislative machinery is geared up to producing laws, and there is no in-built check on this. The drive for legislative rationality must therefore come from outside.

This gives academia a potentially important role. In practice, however, it appears that academics are increasingly involved in departmental work groups, advice committees, EU consultations and are involved in implementation projects. In that role, the interests of the academics run parallel to those of the legislators and politicians. It is then not rational to advise that actually nothing has to be done. Research subsidies for information technology and law show the same divided rationality. (A similar sort of criticism has been expressed with respect to research financed by business. An important difference is that financing by the authorities means financing at the public expense.) Complete transparency is a must in order to make people accountable for money and research results.

An important role could be played by independent supervisors, for example, the national audit office, the ombudsman, the Committee for the Protection of Personal Data. Supervisory bodies could evaluate and criticise the other powers in a general, integrated way. Not only the justification for the

actions would be examined, but also their effectiveness and efficiency. Appointing supervisors could be seen as a confirmation of the increasingly dominant rational model of man expressed by the REMM, their activities as the promotion of rational actions. The supervisory or examining power is not aligned with the legislative power, the executive or the judiciary, but should be seen as a fourth power (Tetras politica, DE MULDER 1997, inaugural speech).

In order to repress phantom legislation, it is recommended that a fourth power should be instituted whose function it will be to evaluate legislation.

With respect to the EU, a high priority should be given to establishing a fourth power whose function is to evaluate legislation, given the multitude of rules and their compulsory character, as well as the relatively large gap between European administrators and the citizens.

In Section 1.7, it is indicated that this study could not say with certainty whether one of the possible explanations, that concerning the lack of familiarity of legislators with information technology (and lack of insight into management), is correct. What can be said is that it takes time before new technology is assimilated in society. Many of the new laws would never have become law if those responsible for them had understood better what information technology really is; an essential step in technology. With respect to some of these laws, they have clearly failed to appreciate the characteristics of fourth generation technology. What is also evident is that some laws do not take into account that people act rationally.

It is recommended that legal studies should be expanded to include a course on 'technology for lawyers' and a course on 'management for lawyers'.