Lee A. Bygrave (ed.)

YULEX 2003

Institutt for rettsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:
Institutt for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 82-7226-077-8
ISSN 1503-5999

unipubskriftserier

Utgitt i samarbeid med Unipub AS
Denne boken går inn i universitets- og høyskolerådets skriftserie
Trykk: AiT e-dit AS
Omslagsdesign Kitty Ensby

1 FORORD

Denne boken er den tredje i Yulex-serien. Siktemålet med serien er å tilby venner av Institutt for rettsinformatikk smakebiter fra ulike temaer som instituttets medarbeidere har vært opptatt av i løpet av dette året. Mesteparten av artiklene i serien er «works in progress» snarere enn ferdigstilte analyser.

Et særlig aktuelt problemområde for forskningen ved instituttet gjelder rettslige konsekvenser ved bruken av elektroniske agenter. *Yulex 2003* er derfor i betydelig grad viet dette problemfeltet.

God jul og fornøyelig lesing inn i det nye året!

Lee A Bygrave

1 PREFACE

This book is the third in the Yulex series. The aim with the series is to offer friends of the Norwegian Research Centre for Computers and Law a "Christmas smorgasbord" of the various themes upon which Centre staff have been working over the past year. The bulk of articles in the series constitute "works in progress" rather than completed analyses.

Of current themes for research at the Centre, the legal consequences of using electronic agents is particularly important. Hence, *Yulex 2003* is devoted in considerable part to that theme.

Merry Christmas and happy reading into the New Year!

Lee A Bygrave

INNHOLD

ELECTRONIC AGENTS AND PUBLIC KEY INFRASTRUCTURE

ROLF RIISNÆS

1 Introduction

It felt good. "Thanks to the electronic agent", he thought, while "Lovely Rita" was fading out on the radio.[1] It was only recently that this became possible. A few years ago it would not have been possible for the radio station to get the soundtrack on the air in such a short time – if the track was available in its collection at all. The radio station was too small to afford an extensive collection of records. Nowadays, the agent technology made available to the station on request and at an affordable price practically any soundtrack. And it could all be arranged from the disc jockey's desk. He would not have to leave the controls to look for a record in the archive.

It was rather unsettling, though, when he thought about there being an "agent" out there, negotiating tracks on behalf of the radio station. What if the agent "turned nuts" and accepted several versions of the same melody or simply kept on negotiating new items? As far as he knew, the agent used by the station had a fairly solid "reputation" and was accepted by most rights managers. If anything went wrong, a lot of problems could easily pile up.

In fact, he and the station relied heavily on the software developers. As far as the disc jockey knew, the agent was basically a piece of software programmed to negotiate licences, with similar agents of right managers around the network, based on instructions from the licensees. To operate the agent, they used two sets of tools: firstly, a software tool used to formalise the instructions comprising the mission of the agent; secondly, the public key infrastructure (PKI) which facilitated the authentication of the agent and its mission. He knew that, even though the tools were not directly related, the functionality of the software tool was based upon the co-existence with the PKI. He wondered how.

---

[1] See the article "Lovely Rita: A Scenario" by Jon Bing and Giovanni Sartor in Jon Bing and Giovanni Sartor (eds), *The Law of Electronic Agents*, CompLex 4/2003 (Oslo: Unipub, 2003), p 11 *et seq.*.

2 The challenges

In the "Lovely Rita" scenario, a public key infrastructure (PKI) is used to secure the communication between the parties. The aim of this article is to take a closer look at how this might be organised. The article does not pretend to provide a description of a system actually in operation; rather to provide a draft proposal for the broad characteristics of a possible solution.

The agents in the scenario operate in an open network, such as the Internet, recognised by the fact that the parties can enter into commercial relations without any prior agreement between them. Undertaking commercial operations in an open network is subject to numerous challenges.[2]

Firstly, there is a lack of transparency in such networks. Any party could operate under any identity or claim any authority on the net, and it is generally difficult to establish whether or not the facts claimed represent the truth.

Secondly, there is a lack of durability in the electronic medium. An electronic message may also be changed without leaving any trace. The combination of these two characteristics may cause evidential problems if a dispute arises.

Thirdly, there is still a lack of tradition and experience in electronic commerce. Traditionally, in commercial relations, one used to have a "gut feeling" with regard to the circumstances under which one could expect a transaction to work. In electronic commerce, one often does not have this feeling. This may result in a lack of trust in electronic commerce as a secure and effective way of doing business.

Fourthly, the computerisation and automated systems require control mechanisms to be formalised. A computer does not (yet) have the ability of a human being to evaluate the available facts of the situation and decide whether it should be considered acceptable or not. The reliability of human intuition with regard to trustworthiness in such relations might be questioned, but in practice we rely heavily on it in day-to-day business practice.

Fifthly, data distributed through the network is potentially being disclosed to others than the intended users.

Finally, it may be necessary to comply with one or more legal requirements.

To a large extent, the challenges are related to the issue of evidence and the matter of trust. The question is: what do the parties need to obtain the level of

---

[2] See, eg, Communication from the EC Commission, "Ensuring security and trust in electronic communication – towards a European framework for digital signatures and encryption", Brussels, 8th October 1997; Bruce Schneier, *Secrets and Lies – Digital Security in a Networked World* (New York: Wiley, 2000).

trust necessary for them to dare completing the transaction? In practice, this should not be expected to be an entirely rational decision based on a careful evaluation of the risks involved and the measures taken. In many cases, it is probably based on common sense and a broad evaluation of the circumstances. Commerce is about managing risks. What is sought is not a "bullet-proof" solution but adequate security at a reasonable cost.

Some basic terminology related to the security requirements should be explained at the outset. First of all, one might want to be able to verify the claimed identity of the party with which/whom one communicates. This functionality is described in terms of "authentication". One might also like to ensure that messages are not changed, accidentally or by purpose, during transmission. This concern relates to "data integrity". Further, one might want to collect proof that a given message was actually sent by a given party – a functionality referred to as "non-repudiation".[3] Finally, one might want to ensure that a message is withheld from any parties that are not authorised to read the message. This concern is about "confidentiality".

3 Public key infrastructure (PKI)

3.1 Public key encryption

Public key infrastructure (PKI) can be regarded as the sum of services constituting the framework for using public key encryption. Public key encryption is encryption based on the use of two different but related keys – one key for encryption and another key for decryption – where it is not possible to compute one key from the other. One key is kept secret to the key-holder (the private key). The other key of the key-pair may be communicated to others (the public key). Digital data encrypted with the public key can only be decrypted with the corresponding private key and the encrypted data are thus kept confidential and will only be accessible to the holder of the private key.

---

[3] This is probably not an accurate use of the term, but it seems it has come to stay. The term was used by cryptographers to express that if one's digital signature algorithm is not breakable, no third party could forge one's signature, thus providing proof that a certain private key was used to sign the message. This does not necessarily provide proof regarding the identity of the sender and, concomitantly, it does not necessarily prevent, in law, the person to whom the private key is formally ascribed, from repudiating the assumption that he/she is the sender of the message in question.

3.2 Digital signatures

To obtain digital signatures the use of the keys is reversed. What is encrypted with the private key can only be decrypted with the public key. Thus, if a message can be decrypted with a person's public key one can be pretty sure that it has been encrypted with the corresponding private key. The encrypted message becomes the "signature" of the sender. The signature is a function of the message so it is also unique to the message.

In real life, the situation is a bit more complicated. What is being signed is actually a one-way hash (ie, mathematical abbreviation or "digital fingerprint") of the message. The result of this operation is appended to the message and this is what is called the "signature".[4]

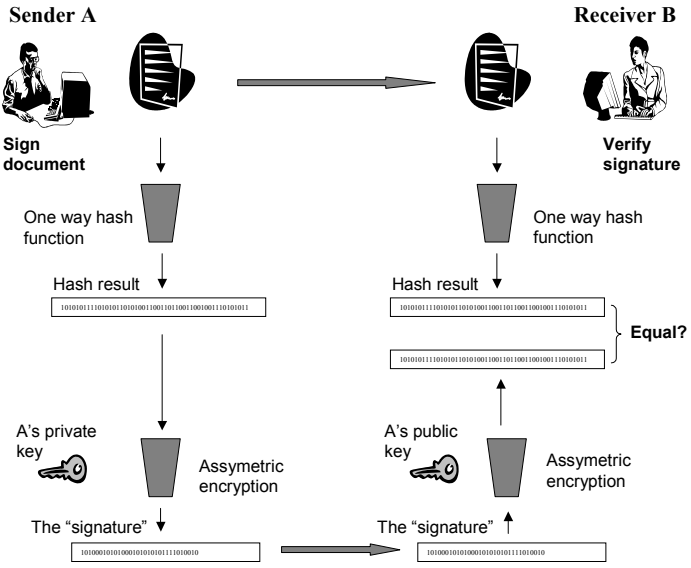


Figure 1: The digital signature process

Also in real life, no one really encrypts a message with a public key (largely because of the relatively lengthy time that such a process usually takes). Operational systems use a hybrid approach combining symmetric and public key

[4] The use of the term "signature" for this purpose is opposed by several commentators. I agree with this criticism. However, use of the term in this context seems to have come to stay. Therefore, focus should now be put on the possibilities and limitations found in the functionality of the technology.

encryption. A standard encryption algorithm is used to encrypt the message with a random key (called a *session key*). That key is encrypted with the public key. As intimated above, the reason for this process is speed.[5] The receiver first decrypts the session key with his private key. Then the message can be decrypted with the session key.

3.3 Trusted services

Among other questions, one may ask: "How do I know who holds the key?" In open systems one possible answer is to introduce a so-called trusted third party (TTP) or certification service provider (CSP) that confirms the association of a public key to a given legal or natural person or electronic agent. In practice, the public key is included in an electronic record called a "certificate" together with some other pieces of information and signed with the digital signature of the service provider. This first issue resolved, there arise several other questions: "How do I know the public key of the service provider so that I can verify the certificate?"; "why should I trust the service provider?"; and "how was the key-holder's identity verified by the service provider?" We shall leave these last questions for now; this article will not treat all the details and problems related to public key encryption and infrastructure. For present purposes, we presuppose that a PKI, trusted by the parties, will be available for the use of electronic agents. The question is how to utilise the PKI.

These remarks notwithstanding, a few comments will be made below on the terms related to, and the use of, *certificates* (see section 3.5).

3.4 Identifiers

The term "identity" is usually related to a natural person and commonly associated with the name of that person. It has been discussed whether this is an appropriate way to use the term with regard to certificates the purpose of which are to distinguish a legal or natural person or electronic agent from other entities.[6] The discussion arises partly because there is no common un-

---

[5] Encryption of the message by the session key, followed by encryption of the session key by the public key, will usually be much quicker than encryption of the entire message by the public key.

[6] See, eg, Roger Clarke, "The Re-Invention of Public Key Infrastructure", December 2001, available from <http://www.anu.edu.au/people/Roger.Clarke/EC/PKIReinv.html>.

derstanding of any globally unique identifier.[7] Further, one might distinguish between "identity", "identifier" and/or "identification data". This discussion will not be entered into here. For present purposes the notions of "identity", "identifier" and "identification data" are used simply to denote data intended to distinguish one entity from other entities.[8] Whether or not such distinctions can be made in a certain transaction depends partly on which data the user already has. For instance, a name and date of birth might be sufficient to distinguish one person from another within a certain user community. However, if the verifier does not know the person's date of birth beforehand, this piece of information will not help him to identify the person.

3.5 Certificates

Broadly speaking, a *certificate* is an electronic record that, by its content, associates certain data with a natural or legal person or an electronic agent.[9] The certificates can be divided into (at least) two categories: (i) certificates that associate a public key with an identifier of a legal or natural person or electronic agent; (ii) certificates that associate an entity with an attribute or role – eg, an authorisation to act on behalf of a legal person or to order payments from a bank account. The first category may be called "ID certificates" or "public key certificates",[10] and the second category "role-based certificates" or "attribute certificates".[11] There are currently few international standards with regard to profiles for attribute certificates but development of such standards is on the agenda of, amongst others, IETF[12] and ETSI[13].

---

7 See, eg, RFC 2693 "SPKI Certificate Theory" and RFC 2692 "SPKI Requirements", both available from <http://www.ietf.org>. See also Carl Ellison and Bruce Schneier, "Ten Risks of PKI: What you're not being told about Public Key Infrastructure", *Computer Security Journal*, vol XVI, no 1, 2000, available from <http://www.counterpane.com/pki-risks.html>; Carl M Ellison, "Establishing Identity Without Certification Authorities", available from <http://world.std.com/~cme/usenix.html>.

8 By "entity" is meant a legal or natural person or an electronic agent.

9 In Directive 1999/93/EC on a Community framework for electronic signatures, the term "certificate" is defined as "an electronic attestation which links signature-verification data to a person and confirms the identity of that person" (Article 2(9)). This excludes certificates related to electronic agents from the ambit of the Directive.

10 Both terms are being used synonymously in this article but the term ID certificate is preferred here because it more directly reflects that the purpose of such certificates in the scenario is to identify the holder of the certificate.

11 The latter is used in this article, see also RFC 3281 "An Internet Attribute Certificate Profile for Authorization" (April 2002) as referenced in the next footnote.

12 The Internet Engineering Task force (IETF) has published a proposed standard protocol RFC 3281 "An Internet Attribute Certificate Profile for Authorization" (April 2002), available from <http://www.ietf.org/rfc/rfc3281.txt>.

The two types of certificates may have the same structure and main characteristics but there are some major differences. Firstly, the attribute certificate does not itself contain a public key. Secondly, the processes of issuing the certificates are different. Given that a person or agent has a trustworthy ID certificate, an attribute certificate can be issued and distributed over the net without any further authentication between the parties. Thirdly, the issuer of the attribute certificate will usually be different from the issuer of the ID certificate. Once a person has an ID certificate, his employer may for instance issue an attribute certificate attesting the relationship with the employee. Fourthly, attribute information usually does not have the same lifetime as an ID certificate. And finally, although ID certificates can be *pseudonymous*,[14] the attribute certificates could be *anonymous* by simply attesting that the holder of a certain key is authorised to perform certain actions without revealing the person's identity. However, the more common approach seems to be to associate the attributes with an identifier.[15]

---

[13] The European Telecommunications Standards Institute (ETSI) has drafted a technical report to identify a set of requirements that will provide a basis on which a subsequent standard can build policy requirements for attributes certified by attribute authorities or certification authorities. See TR 102 044 "Requirements for role and attribute certificates" (December 2002), available from <http://portal.etsi.org/esi/el-sign.asp>.Work by ETSI in the area is done in close co-operation with CEN/ISSS within the European Electronic Signature Standardisation Initiative (EESSI) work programme.

[14] See Directive 1999/93/EC on a Community framework for electronic signatures, Article 8(3) ("… Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name"), and Annex I litra c) ("Qualified certificates must contain: … c) the name of the signatory or a pseudonym, which shall be identified as such").

[15] According to RFC 3281 specification, the attribute certificate links the attributes to an identity, whereby validation of the attribute certificate may require the validation of a chain of public key certificates. The attribute certificate might contain a unique reference to the public key certificate on which it is based (in the "baseCertificateID" field). Alternatively, the attribute certificate may contain an identifier of the certificate holder. This might give the signer freedom to choose which ID certificate (if he has more than one) that should be used to validate the attribute certificate, eg, by different communities. However, the solution faces the problem of matching the identification data of the two certificates. Taking into consideration that the certificates will be issued by different entities, matching the identifiers may not be a trivial task. Consequently, I propose that an attribute certificate preferably be linked directly to an existing public key certificate. Including the "baseCertificateID" in the attribute certificate would in effect render the attribute certificate valid until any one of the two certificates expires or is being revoked. Should the ID certificate be revoked, the attribute certificate can no longer be validated. However, should anonymous attribute certificates be required, the RFC 3281 (7.3) allows the "holder" field to contain, eg, the hash of a public key, in effect confirming the authorisation of the attribute to the holder of the key pair.

The two types of certificates may be used separately or in combination. However, the use of attribute certificates may be more flexible when built on top of existing ID certificates. This flexibility is due to the fact that once a person or agent has the capability of identifying him-/her-/itself over the network by using a certain key (pair), attributes can be attached to the same subject by different entities. An employer will be an authority with regard to issuing attribute certificates to his employees. A bank will be an authority with regard to issuing attribute certificates related to banking services. And a principal will be an authority with regard to issuing an attribute certificate to his agent. In principle, these attribute certificates could be validated using the same pair of keys, which is attested by an ID certificate. This allows the holder to use only one (or, for security reasons, a few) pair(s) of keys, and prove his different roles by way of the attribute certificate relevant to the transaction in question. Different user communities might develop community-specific attribute profiles. The music industry, for instance, could specify a profile – eg, within the specifications of RFC 3281 – containing the attributes required to authorise agents to negotiate licences as described below (see section 4).

Yet we also have to make another distinction between different types of certificates. This is related to "key-usage". For security purposes, it is recommended not to use the same pair of keys for operations such as encryption, authentication and digitally "signing" electronic records. We will not go here into a detailed explanation of this. The recommendation for different key pairs is reflected in standards for certificate policies and profiles. There is a field in the certificate called "key-usage" dedicated to distinguishing between the different uses. Key-usage should be set to "encryption" if the public key is to be used for encryption purposes. It should be set to "non-repudiation" when the related key-pair is intended for "signing" contracts etc. If it is set to "digital signature", it is intended for authentication purposes only. A key with a certificate marked "digital signature" should not be used to sign, or enter into, so-called "legally binding" instruments or transactions. The reason is that the authentication key might be used to sign so-called "challenges" (a random string of bits to be signed for authentication purposes) and the signer will not necessarily know what he is signing. Consequently, a "signature" based on an authentication certificate can more easily be disputed, with the signor claiming that he did not have an intention to be bound and that he did not know what he was signing. It would seem to be an open question whether or not it has any legal significance if the certificate is set for "non-repudiation" or "digital signature" when it comes to a concrete transaction.

4 PKI as applied to the scenario

4.1 Introduction

The following is a proposal for one possible way of organising the use of PKI for electronic agents. We will not discuss in depth whether or not PKI is the best solution for the scenario, neither all the issues related to the proper operation of the PKI. However, given such proper operation, it is my view, that PKI is an efficient way of securing the electronic communication between the parties to the scenario. First and foremost, because the certificates may, in principle, hold all data necessary to verify the transaction, it may be processed automatically by agent technology and the current status of the certificate may be verified on request.

The idea of this article is that certificates are used to formalise and carry the data necessary to verify the identity of the agents, the licensee, the right holders and the right managers. Certificates could also be used to formalise the relationship between the agent and the licensee even when it is a dynamic relation, and to protect data during transmission.

There are presumably few legal obstacles towards the use of PKI for electronic agents. Exporting encryption technology is subject to export restrictions under the so-called "dual goods" regulations issued pursuant to the Wassenaar Arrangement. However, these regulations have recently been revised and do not represent an obstacle to the use of "off-the-shelf" public key encryption technology for commercial purposes.

There are few requirements as to form with regard to license agreements. The question of whether, and on what basis, an agent may enter into license agreements on behalf of the licensee will not be discussed here. For the purpose of this article, it is presupposed that an agent may enter into a contract in electronic form that binds the licensee.

From here on, the principal question is whether or not certificates and PKI are adequate measures to build trust between the parties and for the interoperability of agents.

4.2 Identifying and authorising the parties

It will be recalled that the certificate could be described as an electronic record that associates a public key with an identifier or an attribute of a person, organisation or electronic agent.[16]

The software used to register the instructions for the agent could also be a piece of "certificate issuer software". An extract of the instructions could be represented in a certificate – an attribute certificate – to be associated with the agent. Somehow, the attributes have to be linked to an authentication mechanism held by the agent, preferably a public key. The public key could, in principle, either be held by the agent permanently or assigned to it by the radio station as a part of a single purpose key-pair.

When we say that an agent holds a public key or an electronic signature, we mean that the piece of software comprising the agent is equipped to utilise a public-key encryption system during its communication processes. We mean further that a public key in a certain certificate is related to the private key used by the agent.

Let us call the agent "Muzak" and the rights manager "ERM". The name of the radio station is "Radio West".

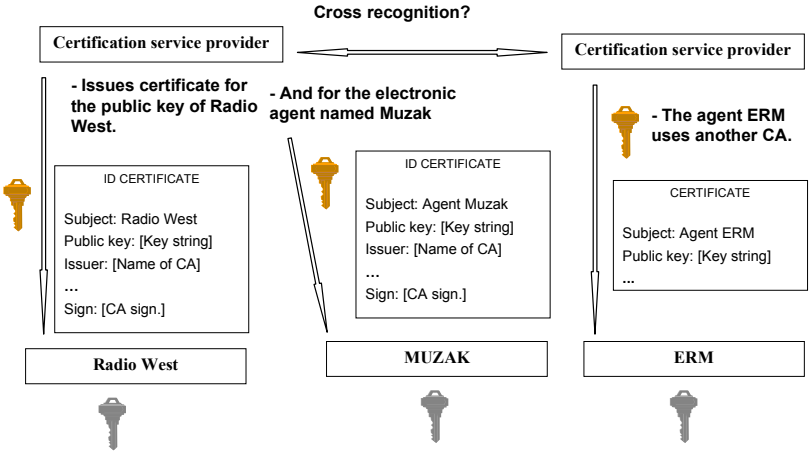
We assume that the agent is operating from a server and that it has more clients than just our radio station. In this case, it looks like the more efficient solution to let the agent have its own pair of keys, with a certificate associating the public key with the agent named Muzak. Although the agent could be hired on-line, the certificate may also be related to an organisation providing access to the services of the agent. Somewhere down the line, an organisation or natural person will pick up the payment for the services of the agent. Given that the agent holds such a certificate, it could be identified by users on-line – eg, as an agent recognised by rights-managers on the net.

It would also make it easier to issue attribute certificates to the agent by the users, because linking the attribute certificate to the ID certificate of the agent authorises in effect the key already certified to be that of the agent. Given that the users trust the ID certificate, they will not have to bother with proof of possession of keys or other authentication mechanisms with the agent when issuing their attribute certificate.

The agent may even have a certain "reputation" in the networked society. For instance, it may be general knowledge that the agent only negotiates certified missions or that the agent (or rather its provider) guarantees pay-

[16] ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates" is limited to natural persons, while ETSI TS 102 042 "Policy requirements for certification authorities issuing public key certificates" supports certificates even for automated systems. Both policies are available from <http://portal.etsi.org/esi/el-sign.asp>.

ment etc. Such reputation requires an ability to uniquely identify the agent over a period of time.



Once a potential user of the agent has identified a certificate as belonging to the agent, the attribute certificate could be issued, attesting that the rightful holder of the ID certificate, and consequently the key certified by the certificate, is authorised to negotiate a piece of music on its behalf. The certificate may contain, eg, a statement that the user will consider itself bound by licences negotiated by the agent and other relevant data about the user. The music industry may develop community-specific certificate profiles for this purpose within the specifications of existing standards, such as RFC 3281 (see above). When an attribute certificate is related to an existing ID certificate, the attribute certificate can be validated until either certificate expires or is being withdrawn.

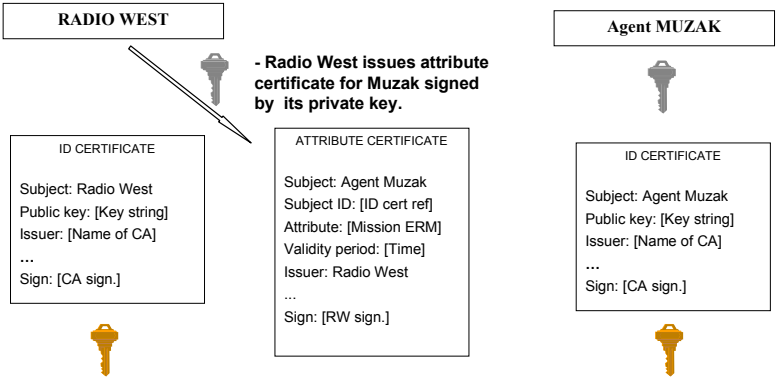
Like the agent, the radio station needs to have a certificate of its own. One could, of course, use the producer's personal certificate to initiate the process, but the receiver of such a certificate would not necessarily be able to identify him as authorised to hire the agent on behalf of the radio. Therefore, an *organisational certificate* seems to be more appropriate. Such a certificate confirms that a certain public key be associated with the radio station as such. The private key of the radio station could be permanently installed on its computer system and activated only when authorised software was used and the user properly authenticated. For now, we disregard the further problems of securing the private key.

4.3 The mission

The producer opens an application to register the requested piece of music. During the registration process, he has access to certain databases containing data that are relevant to the agent's mission, such as the object identifier of the work. When registration is complete, he is prompted by the application to activate the private key of the radio station in order to "sign" the mission. He authenticates himself for the system – eg, by way of a password to access the private key.

The outcome of the registration process is probably twofold. Firstly, there will be directions to be processed by Muzak, and secondly there will be an attribute certificate which Muzak may "present" to ERM to prove that he has a mission on behalf of the radio station. The private key of the radio station is used to "sign" the attribute certificate and the Radio West's ID certificate is attached.

The attribute certificate contains information such as the identifier of Muzak's ID certificate, the identifier of Radio West as issuer, a statement that Muzak is authorised to negotiate works on behalf of Radio West and the signature of the issuer. It also contains a statement on the period during which the certificate is going to be valid. In this case, the validity period will probably just be a couple of minutes long. If the negotiations do not succeed within this relatively short time frame, another listener will be on the line and the idea of playing "Lovely Rita" will be obsolete. Consequently there is no need for a revocation service for the attribute certificate. It will invalidate itself by its contents long before revocation could be made effective.

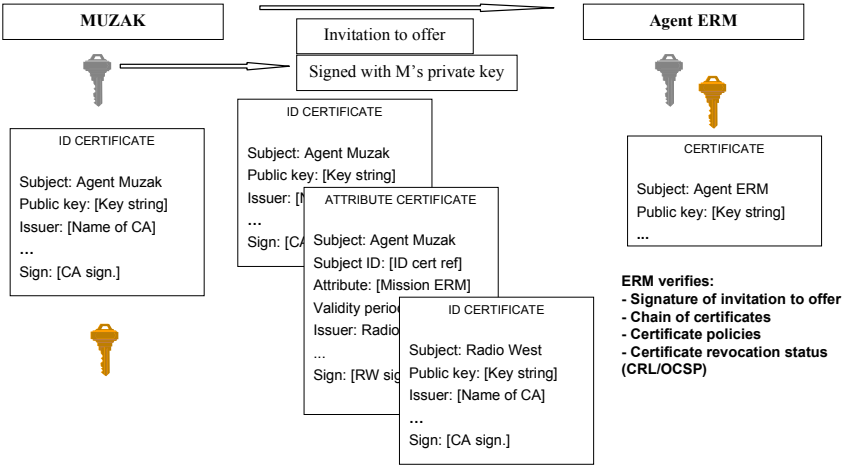


The certificate might also, in principle, hold information such as the identifier of the song for which a licence is to be negotiated and data on how payment is to be arranged. Perhaps Radio West might offer eCash. Or, more likely for a radio station, it will offer settlement by account with a clearing-house commonly used in the business.

4.4 Negotiations

The agent approaches the other agents on the net, negotiates the terms and decides on a solution as described in the scenario. The agents may identify each other prior to starting the negotiations but more likely when entering into the license agreement. At least when it comes to checking revocation status of the ID certificates (if considered necessary), it does not seem to make sense to check alot of certificates from different agents when only one will be party to the contract. There is a risk, of course, that the transaction is overturned if the certificate is not accepted. A compromise would be to verify that the agents hold certificate types that Muzak is allowed to accept, but to postpone the process of verifying the validity of the certificates.

To verify that a certain agent is associated with a key, the agent will have to "sign" a set of data known to the verifier. This could be a "challenge" sent from the verifier or, eg, an offer. Yet one can never identify someone else just by reading the certificate. Given that the agents negotiate by exchanging offers and counter-offers, the signatures on such offers might identify the agents by way of the certificates.



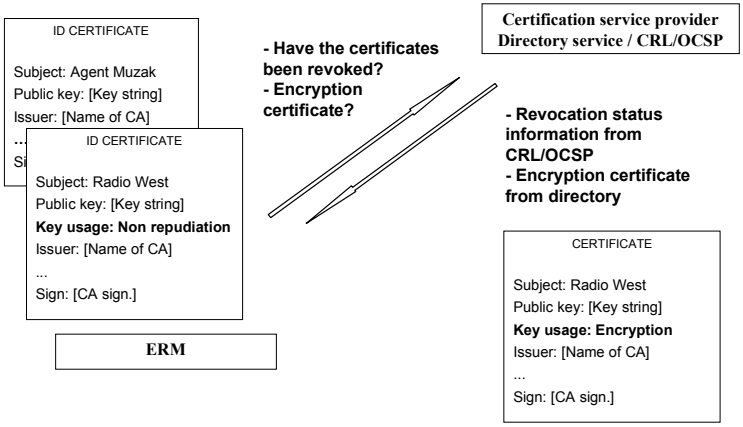
Let it be presumed that Muzak provides an invitation to offer. The invitation is signed and Muzak attaches the attribute certificate together with its own ID certificate and the ID certificate of the radio station containing the key necessary to verify the attribute certificate.

Even though no revocation service is needed for the attribute certificate, ERM (the agent of the right manager) might want to verify that the certificate of the radio station is still valid, otherwise the attribute certificate could be a falsification. The validity question probably would not matter much with regard to this transaction. The request is for a very limited licence. Yet greater values might be at stake. The revocation status service will be referenced in the certificate – eg, by way of an URI.

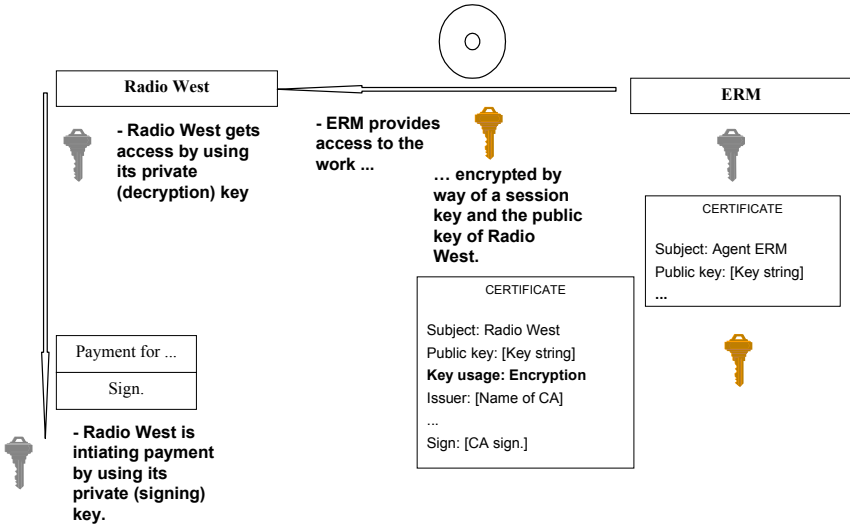
It will be seen that that in this scenario there do not exist any signatures related to natural persons. This probably does not matter. There are, as far as we know, no legal requirements for contracts or mission statements to be in writing, to be signed etc. The signatures and certificates of the radio station and the agent may not have any independent legal significance. Yet they engender trust between the parties. Given that the agents succeed with the required verifications, the parties can be relatively sure that the transaction and payment can be fulfilled securely. Nevertheless, without entering into the issue of agency law and the question of an electronic agent in that capacity, we may reflect over the fact that the attribute certificate looks very much like a written power of authorisation.

4.5 Completing the contract

Once the contract is completed, a copy of the work should be transmitted to Radio West. Even though ERM did not bother to check on revocation of the certificates earlier, ERM might want to look up the encryption certificate of Radio West. The risk of entering into a contract based on a falsified certificate does not bother him, but he would not like to distribute a copy of the work, under a limited licence, to anyone. Perhaps he wants to make sure that it is really a radio station that receives the work, expecting them to respect the limited licence or using equipment that does. For a private person, streaming would perhaps be the adequate measure of licensing.



So, based on the identity certificate of Radio West, ERM looks up the corresponding encryption certificate from the database of the certification service provider. Having verified that it has not been revoked, and that it actually belongs to a registered radio station, ERM prompts the database that holds the work to encrypt and transmit a copy. The work is collected, a session key is calculated and the work encrypted. The session key is encrypted with the public key from the encryption certificate. The lot is ready for downloading by Radio West. The copy will be released as soon as payment is made or the clearing-house confirms settlement.



4.6 Closing

Piip! The agent made it! A dialogue box tells the producer that the licence was somewhat more extensive than required, but the price is reasonable. The producer clicks the “download” button. This prompts a payment order, signed of course, the work is then released and the piece is ready to go live. The work might also be downloaded automatically subject to the agent authorising the payment. Organising the payment, though, is beyond the scope of this article.

ELECTRONIC AGENTS AND CONTRACT PERFORMANCE: GOOD FAITH AND FAIR DEALING[1]

EMILY M WEITZENBÖCK

Abstract

This paper examines how the civil law principle of good faith and the common law notion of fair dealing apply during the performance of contracts. After a brief look at their application in the precontractual stage, there is an examination of the notion of good faith and fair dealing in contract performance. Reference is made to the duty of the parties to act loyally and to cooperate during the performance of the contract. An argument is made for an objective interpretation of good faith which will enable its application to electronic agents.

1 Introduction

Electronic agents are playing an increasingly active role in the negotiation, formation and execution of contracts. A fundamental characteristic of electronic agents which distinguishes them from other software agents is their

---

[1] This paper was originally presented in slightly different format at the first LEA (Law and Electronic Agents) workshop on "The Law of Electronic Agents" held in Bologna in July 2002 in connection with the AAMAS (Autonomous Agents and Multi-Agent Systems) 2002 Conference, and is reproduced in the proceedings of this workshop: see *The Law of Electronic Agents: Selected Revised Papers*, LEA Workshop on the Law of Electronic Agents, CIRSFID (Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica), University of Bologna, 2002, pp 67–73. The paper was partly developed within the project ALFEBIITE (A Logical Framework for Ethical Behaviour between Infohabitants in the Information Trading Economy of the Universal Information Ecosystem; IST-1999-10298), funded by the European Commission. The paper is the sole responsibility of the author and does not represent the opinion of the European Community. The Community is not responsible for any use that might be made of the content of the paper.

autonomy. Such agents operate without the direct intervention of human beings or other agents, and have some degree of control over their actions and internal states [Russell & Norvig 1995].[2]

Some of the issues being discussed in a number of disciplines such as Computer Science, Cognitive Science and Logic are how such agents should behave in order to fulfil their contractual obligations, with issues like trust and security at the forefront. Legal norms may also regulate the behaviour of contracting parties both during the negotiation and contract formation stage and also, once a contract has been concluded, in its performance or execution stage, by the imposition of certain standards of behaviour which the parties should follow. An important criterion for contractual behaviour in civil law systems is the requirement that parties should negotiate, conclude and carry out contracts in good faith (*bona fides*). In common law countries, there is no general rule requiring the parties to conform to good faith. English jurists prefer the term "fair dealing" – a term which appears to encapsulate a more objective test of fairness, to pragmatic, common law lawyers.[3]

This paper is part of ongoing research on the role of good faith and fair dealing in contract formation and performance. After briefly touching upon this duty in the **precontractual** stage, it focuses on the principle of good faith and fair dealing in the **performance** stage of the contract, with a view to establishing what standards of behaviour are legally expected and required at that stage.[4] It is presumed that where contracts are to be negotiated and performed by electronic agents, such agents would need to conform to these standards of behaviour. Nowadays, it is not only possible for agents to actually negotiate and conclude contracts on behalf of a party – a fact recognised expressly in the legislation of some countries[5] – but also to perform part or, in some cases, even all of that party's obligations in the contract. For example, where the object of the contract is the delivery of a digital product, the

---

[2] According to Russell & Norvig [1995, p 35], "[a]n agent's behaviour can be based on both its experience and the built-in knowledge used in constructing the agent for the particular environment in which it operates. A system is autonomous to the extent that its behaviour is determined by its own experiences."

[3] According to American jurists, the requirement of good faith in American law – similar to English law – does not apply to contract negotiations.

[4] For a more detailed study on the role of good faith and fair dealing at the precontractual or contract formation stage, see Weitzenböck [2002].

[5] Thus, the US Uniform Electronic Transactions Act (1999) in section 14(1) provides that "a contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements." A similar provision is found in the US Uniform Computer Information Transactions Act (1999) (section 107) and in Canada's Uniform Electronic Commerce Act (1999) (section 21).

contract may be performed by the agent where the product is delivered electronically to the user upon instruction by the electronic agent.

2 Precontractual duties of good faith and fair dealing

Before proceeding further with the discussion on contract performance, some comments will be made on the applicability of the good faith principle to the contract formation stage. It should be stated at the outset that both civil and common law systems regard the freedom of the contracting parties as sacrosanct. Parties should be free to decide whether to enter into contractual relations or not. However, what happens when, because of certain blameworthy conduct of a contracting party at the precontractual stage, the contract is invalid or not perfected? A number of civil jurisdictions such as Germany and Italy developed the doctrine of *culpa in contrahendo* which is based on the notion that damages should be recoverable against the party whose blameworthy conduct during negotiations for a contract brought about its invalidity or prevented its perfection [Kessler & Fine 1964]. As a consequence of the good faith principle, one may identify the development of a number of standards for precontractual behaviour [Weitzenböck 2002]:

- the development of certain duties of disclosure (*obligations d'information*) in virtue of which, having regard to the subject matter of the contract and the obligation undertaken, there should be disclosed certain relevant information which only one party knows and which the other party could not have otherwise found out;
- the development of the notion of precontractual liability where (i) there is a sudden and unjustified rupture of negotiations, or (ii) the contract is not concluded because one of the parties had no real intention to contract: in such cases, the court takes into account whether the other party had incurred expenses in preparation and in the expectation of concluding the contract.

English law does not recognise a general duty to negotiate or to perform contracts in good faith [Whittaker & Zimmermann 2000]. Nevertheless, it has been held that though "English law has, characteristically, committed itself to no such overriding principle … [it] has developed piecemeal solutions in response to demonstrated problems of unfairness".[6] English legal writers hold that there is no duty of disclosure at the stage of contract negotiation,

[6] *Interfoto Picture Library Ltd v Stilletto Visual Programmes Ltd* (1989) 1 QB 433, 439.

save in the case of fiduciary contracts (eg, insurance, suretyship). However, where this amounts to fraudulent representation or negligent misstatement, a remedy would be available in tort. Moreover, when negotiations have led to the conclusion of a contract, the silence of one party could be problematic for such party (who could be liable for damages and/or find the contract rescinded) where the information suppressed relates to a fact that is deemed to be an implied term. Harrison [1997] puts forward the thesis that the duty of good faith or fair dealing as it applies in the formation of contracts of sale, is normally a twin duty of *candour and accuracy*. This is the duty to give proper information or none at all about what is being sold in contracts outside the area of fiduciary contracts. Harrison states that this is a presumption of law and operates both as an obligation in interpreting the contract and as an additional implied term where there are no relevant express terms to be interpreted. She holds that it does not operate as regards matters which it would be normal and possible for the buyer to investigate himself. Most importantly, Harrison states that a precontractual breach of this duty *has no effect unless a contract is made*. Thus, the effect on the parties only occurs when a contract is made, but not if negotiations break down.

In the case of a sudden and unjustified rupture of negotiations or where the contract is not concluded because one of the parties had no real intention to contract, common law judges have also ingeniously provided a basis for recovery, without entering into the notion of good faith, by using the different notions of collateral contact, restitution and the law of torts. In fact, Cohen [1995] affirms that the collateral contract and the tort of negligence currently serve as the main tools for imposing precontractual liability. As Furmston *et al* [1998] explain, whether or not common law courts ultimately embrace good faith, there is an inherent strength in the common law to police bad faith.[7]

In the subsequent section, it is examined whether one can also trace similar criteria for behaviour during contract performance.

3 Good faith and fair dealing in contract performance

3.1 The civil law notion of good faith

The notion of good faith originates in Roman law where it added an element to *iudicia stricta* (strict law) which enabled a court to take into account cir-

[7] Furmston *et al* [1998] are here referring to English and Australian common law.

cumstances, defences and considerations of fairness which might otherwise have been excluded.

In Germany, it is linked with the notion of *Treu und Glauben* and is enshrined in §242 of the *Bürgerliches Gesetzbuch* (BGB) which provides in general terms that the debtor is bound to perform according to the requirements of good faith, taking into consideration general practice in commerce. Whittaker & Zimmermann [2000, p 39] explain this notion thus: "'Treue' … signifies faithfulness, loyalty, fidelity, reliability; 'Glaube' means belief in the sense of faith or reliance. The combination of 'Treu und Glauben' is sometimes seen to transcend the sum of its components and is widely understood as a conceptual entity. It suggests a standard of honest, loyal and considerate behaviour, of acting with due regard for the interests of the other party, and it implies and comprises the protection of reasonable reliance. Thus it is not a legal rule with specific requirements that have to be checked but may be called an 'open' norm. Its content cannot be established in an abstract manner but takes shape only by the way in which it is applied."

This provision had a profound effect on the development of German contract law by the courts who created a number of obligations to ensure a loyal performance of a contract such as a duty of the parties to co-operate, to protect each other's interests and to give information.

In France, according to article 1134, para 3 of the *Code Civil*, contracts must be performed in good faith. Though the French courts have not given the notion of *bonne foi* the same importance as the German courts, similar results were obtained by the application of a general theory of *abus de droît* which was developed at the end of the 19th century and was based on good faith. Performance of contracts in good faith has been interpreted by French jurists as implying two duties on the contracting parties: (i) a duty to act loyally (*obligation de loyauté*); and (ii) a duty to co-operate (*devour de coopération*) [Weill & Terré 1986]. These duties are discussed in more detail in section 3.1.1 below.

Similarly, according to the Italian Civil Code, good faith is required in the negotiation (art 1337) and performance (art 1375) of the contract. Article 1175 dealing with obligations in general provides that the debtor and creditor shall behave in accordance with the rules of fairness (*correttezza*). According to Galgano, the requirement of good faith is the duty of contracting parties to behave "*con correttezza e lealtà*" [Galgano 1985, p 327].

Some words should also be said about the current trend in the European Union and internationally. The Principles of European Contract law impose a duty of good faith in the formation, performance and enforcement of the parties' duties under a contract. Article 1:201 provides that:

(1) Each party must act in accordance with good faith and fair dealing.
(2) The parties may not exclude or limit this duty.

The Principles of International Commercial Contracts issued by UNIDROIT (International Institute for the Unification of Private Law) in 1994 have a similar provision to Article 1:201.[8] As a corollary of good faith, Article 1:202 of the Principles of European Contract Law imposes on each party "a duty to co-operate in order to give full effect to the contract". Though these Principles do not have the binding force of either national law or international treaties or conventions, they aim to suggest a modern European *lex mercatoria* and to help bring about harmonisation of general contract law within the European Union [Lando & Beale 2000].

3.1.1 An impossible criterion for electronic agents?

From the above discussion on the meaning of the principle of good faith in civil law countries, where terms such as "honesty", "faithfulness", "loyalty", "fidelity" and "reliability" are used, it may appear difficult to envisage how such characteristics could be portrayed by electronic agents. They tend to point to the state of mind of the individual contracting party. However, if one looks more closely at how this principle has been interpreted in certain civil law countries, such as France and Italy, one finds that very often, objective criteria have been set by the court.

Italian writers point out that good faith and fair dealing are *objective* concepts which refer to the behaviour of the honest businessman.[9] Levanti [2001] links *buona fede* during the performance of the contract with the notion of abuse of rights and holds that there is a negative and a positive duty on each of the parties: a negative duty not to abuse of one's position so as not to unjustly aggravate the situation of the other party, and a positive duty to safeguard the contract's usefulness for the other party insofar as this does not import an appreciable sacrifice of one's reasons for contracting.[10]

---

[8] Article 1.7 provides: "(1) Each party must act in accordance with good faith and fair dealing in international trade. (2) The parties may not exclude or limit this duty."

[9] See further on this, Betti, *Teoria generale delle obbligazioni*, Volume I (1953), cited by Lando & Beale [2000].

[10] Levanti [2001] explains these twin duties as "[il] dovere (negativo) di non abusare della propria posizione al fine di non aggravare ingiustificatamente la condizione della controparte, nonché … nel dovere (positivo) di attivarsi per salvaguardare l'utilità della controparte nei limiti in cui ciò non comporti un apprezzabile sacrificio delle proprie ragioni." She holds that "si è visto nella violazione della buona fede un indice sintomatico di abuso del diritto, sanzionato nelle forme tipiche della responsabilità contrattuale o, talora, attraverso rimedi che potremmo definire di 'esecuzione in forma specifica'."

In France, in assessing whether the debtor of an obligation – the person who has to execute the obligation forming the object of the contract – has acted loyally, the court will examine whether he acted as a *bonus paterfamilias* [Weill & Terré 1986]. This is a familiar objective legal standard in civil law jurisprudence which measures behaviour by considering whether a good "father of a family"[11] would have behaved in such a manner. Reference is made to the aim or object of the contract. If the behaviour of the debtor has permitted the attainment of such object, then he cannot be said to have acted in breach of good faith, even if the actual performance does not conform strictly to the contractual stipulations. This means that the debtor should abstain from *dol* which here amounts to fraud.

The creditor of an obligation is also bound by the duty to act loyally. He must abstain from bad faith (*dol*), disloyalty, and from manoeuvres which will make the performance of the contract impossible or more onerous for the debtor. He is also deemed to be in breach of his duty of loyalty if, on the pretext of conforming with the execution, he imposes on the debtor pecuniary hardships which are disproportionate to the usefulness of the object which the contract is aimed to achieve. Therefore, he should refrain from causing the debtor useless expenses. For example, French jurisprudence has held that a carrier should send merchandise on the itinerary which is most advantageous for the shipper [Weill & Terré 1986].

The duty to co-operate is linked with the duty of disclosure (*obligation de renseignement*) in virtue of which one party may be deemed to have a duty to bring to the knowledge of the other party certain facts which he has an interest to know in order to perform the contract. For example, jurisprudence in France has held that the manufacturer or the seller of a piece of equipment should indicate its mode of use and the dangers that its use may bring. Similarly, the lessor should inform the lessee about known defects in the property leased [Weill & Terré 1986]. The duty to co-operate also implies the obligation that each party has to facilitate the performance of the contract by the other party. For example, in a publishing contract, the author must correct the proofs and return them.

[11] This use of the term here is similar to the test of the reasonable man in common law jurisdictions.

3.2 Good faith or fair dealing in common law?

The existence of an objective criterion – besides a subjective one – in the notion of good faith is also acknowledged by Steyn LJ [1997, p 438], who, writing extra-judicially, observes that: "Undoubtedly, good faith has a subjective requirement: the threshold requirement is that the party must act honestly. That is an unsurprising requirement and poses no difficulty for the English legal system. But good faith additionally sets an objective standard, viz. the observance of reasonable commercial standards of fair dealing in the conclusion and performance of the transaction concerned. […] Used in this sense, judges in the greater part of the industrialised world usually have no great difficulty in identifying a case of bad faith. It is not clear why it should perplex judges brought up in the English tradition."

He concludes that "there is not a world of difference between the objective requirement of good faith and the reasonable expectations of parties".

This is also the case in the United States. The Uniform Commercial Code (UCC) of 1960 provides in section 1-203 that "[e]very contract … imposes an obligation of good faith in its performance or enforcement." This is mirrored in §205 of the Restatement of Contracts Second[12] which states that "[e]very contract imposes upon each party a duty of good faith and fair dealing in its performance and its enforcement." Good faith is defined in the UCC as "honesty in fact in the conduct or transaction concerned".[13] In the case of a merchant, the UCC provides that good faith means "honesty in fact and the observance of reasonable commercial standards of fair dealing in the trade."[14] The emphasis here is on *conduct* and not on (subjective) intentions.

3.3 Focus on the objective requirement of good faith

It is submitted that the answer to the difficulty raised above, with regards to how electronic agents may fulfil the requirements of good faith and fair dealing, lies in focusing on the *objective* requirement of good faith. This approach has the advantage of focusing the inquiry on whether the agent has observed reasonable commercial standards of fair dealing in the negotiation and performance of the contract. In the case of contract performance, the twin duties of loyalty and co-operation should be given an objective interpre-

[12] The Restatement Second was introduced in 1979 with official promulgation in 1981.
[13] See §1-201(19) of the UCC.
[14] See §2-103(1)(b) of the UCC.

tation, an approach already adopted in a number of civil law countries – as discussed above. Electronic agents perhaps also need to reach a more sophisticated technological level that enables them to operate on the basis of rules developed on these objective criteria.

4 Final considerations

In a discussion of the notions of good faith and fair dealing in contract performance by electronic agents, one should not forget that the general tendency of courts and of the legislator is to attribute the acts of the electronic agent to the user who activated it and to view the electronic agent as a tool of the user. This is in spite of the fact that the user may not have been directly involved or "consulted" by the electronic agent in the performance of the contract.[15] It is not unlikely to envisage that a court may put weight on the user's actual *choice* of an electronic agent for a particular purpose. It could thus appear to the court that a user who selects a cheap, off-the-shelf software agent for a high-risk, high-value transaction is not in good faith. However, users may find it difficult to determine what kind of electronic agent system they should use, and may consider the burden of such a decision too onerous. If there is to be more widespread use of electronic agents, consumers must have confidence in the technology. This means that there is need for the constant development of more secure and reliable agent systems that take into account the above-mentioned good faith factors. Some authors [Stuurman & Wijnands 2001] have even advocated the development of a security classification and the certification of agents by reference to a particular class of security standards. Requirements could then be imposed in respect of the security level which the agent must fulfil if it is to be authorised or accepted for certain activities.[16]

---

[15] See, eg, section 107 of the US Uniform Computer Information Transactions Act (1999) which provides that a person that uses an electronic agent "is bound by the operations of the electronic agent, even if no individual was aware of or reviewed the agent's operations or the results of the operations."

[16] Such a system may require monitoring to determine whether the agent complies with the specified level of security. This may lead, in turn, to the development of a system of independent verification marks for agent security features. Karnow [1997, p 178] has proposed the introduction of a certification system for electronic agents, in virtue of which agents could only be used after they have been certified. Another author [Lerouge 2000] has suggested voluntary labelling systems.

References

N Cohen (1995), "Pre-contractual duties: Two freedoms and the contract to negotiate", in J Beatson & D Friedmann (eds), *Good Faith and Fault in Contract Law* (Oxford: Clarendon Press).

M Furmston, T Norisada, J Poole (1998), *Contract Formation and Letters of Intent* (Chichester: John Wiley & Sons).

F Galgano (1985), *Diritto Privato* (Padova: Casa Editrice Dott. Antonio Milani, 3rd ed).

R Harrison (1997), *Good Faith in Sales* (London: Sweet & Maxwell).

CEA Karnow (1997), *Future Codes: Essays in Advanced Computer Technology and Law* Boston / London: Artech House).

F Kessler & E Fine (1964), "'Culpa in contrahendo', Bargaining in Good Faith and Freedom of Contract: A Comparative Study", *Harvard Law Review*, vol 77, pp 401–449.

O Lando & H Beale (2000), *Principles of European Contract Law – Parts I and II combined and revised* (The Hague / London / Boston: Kluwer Law International).

JF Lerouge (2000), "The use of electronic agents questioned under contractual law: Suggested solutions on a European and American Level", *The John Marshall Journal of Computer & Information Law*, vol XVIII, pp 403–433.

S Levanti (2001), "Abuso del Diritto", *Diritto & Diritti*, June 2001, at <http://www.diritto.it/articoli/civile/levanti.html> (last visited 25.11.2003).

SJ Russell & P Norvig (1995), *Artificial Intelligence: A modern approach* (New Jersey: Prentice Hall).

Steyn LJ (1997), "Contract law: Fulfilling the reasonable expectations of honest men", *Law Quarterly Review*, vol 113, pp 433–442.

K Stuurman & H Wijnands (2001), "Intelligent Agents: a curse or a blessing? A survey of the legal aspects of the application of intelligent software systems", *Computer Law & Security Report*, vol 17, pp 92–100.

A Weill & F Terré (1986), *Cahiers Dalloz – Droit Civil: Les Obligations* Paris: Dalloz, 4th ed), pp 359–362.

EM Weitzenböck, "Good Faith and Fair Dealing in the Context of Contract Formation by Electronic Agents", *Proceedings of the AISB 2002 Symposium on Intelligent Agents in Virtual Markets*, 3–5 April 2002, Imperial College of Science, Technology & Medicine, University of London.

S Whittaker & R Zimmermann (2000), "Good faith in European contract law: surveying the legal landscape", in R Zimmermann & S Whittaker (eds), *Good Faith in European Contract Law* (Cambridge: Cambridge University Press), pp 7–62.

NETTETS URINNVÅNERE

JON BING

Når vi ser tilbake, virker kanskje debatten omkring definisjonen av elektroniske agenter som personer som en storm i et vannglass.

Autonome, elektroniske agenter er de velkjente «hjelperne» som i form av datamaskinprogrammer bistår brukere på Nettet. Historisk sett vokste de frem fra det som i begynnelsen ble kalt «søkemotorer». Dette var programmer identifiserte nettsider, og foretok en rudimentær analyse av innholdet ved hjelp av de elementene i en nettside som er overskrifter, sammendrag av innhold osv. Dette ble brukt som grunnlag for å etablere indekser. Ved å søke på stikkord, ville en bruker få henvisning til sider som var karakterisert med det eller de ord som ble angitt. Ved å klikke på henvisningen, ble det etablert forbindelse med den siden som det var henvist til.

Dette virker selvsagt tungvint og omstendelig sammenlignet med dagens teknologi. Men det inneholdt kimen til virkelige elektroniske agenter – programmet som samlet inn stikkordene, var på en måte en slik elektronisk agent.

Naturligvis kom det først fart i utviklingen da agenter for alvor ble tatt i bruk for elektronisk handel. Skulle man f eks kjøpe en flyreise, brukte man en «reiseagent». En tidlig populær versjon av en slik agent i Norge var REISEBOT levert av det tyske selskapet NullNullSieben. Når brukeren skaffet seg en personlig agent, ville den gjennom en dialog registrere brukerens preferanser – f eks om graden av komfort på flyreisen, fortrukne selskap, flyplasser brukeren helst ville unngå ved mellomlandinger osv. Når brukeren så bestilte billett, ble bare reisemålet angitt sammen med den aktuelle reisedatoen. Så ordnet agenten resten. Den ville – bak kulissene, så å si – ta kontakt med aktuelle flyselskaper, sammenligne priser og reiseruter og oppta forhandlinger med de agenter som representerte reiseoperatører. Agentens programmer tillot forhandlinger, og mange variabler som brukeren kanskje ikke tenkte på, kunne trekkes inn – for eksempel flyselskapets sikkerhet, erfaringer med overbooking, kvalitet på måltider og lignende forhold. Agenter utvekslet data seg imellom, slik ville agenter som representerte kunder for eksempel danne seg en «oppfatning» (agenter ble allerede den

gangen beskrevet med ord som metaforisk omtalte dem som personer) om i hvilken grad man kunne stole på agenter som representerte flyselskaper.

Sett fra brukerens side, fortonet det hele seg enkelt. Brukeren bare aktiverte agenten, og kort tid etter bekreftet agenten at reisen var bestilt, anga reiseplanen og knyttet en elektronisk billett til det smartkortet brukeren hadde angitt. Sperreilden av meldinger som agenten initierte for å gjennomføre forhandlingene og transaksjonen, var usynlige for den vanlige bruker.

Bruken av agenter utviklet seg raskt, og etter 2010 skjedde de aller fleste transaksjoner på Nettet ved bruk av agenter. Agenter organiserte fjernsynsprogrammer og leide filmer, ladet musikkanlegget, hentet frem nyhetsstoff fra ulike kilder – i det hele bisto brukeren ved kjøp av all slags tjenester og varer.

Men nettopp fordi agentene fikk stadig mer sofistikerte programmer for forhandling og kommunikasjon med andre agenter, hendte det av og til at resultatet overrasket brukeren. Plutselig var flyturen Oslo-Roma bestilt via Moskva: Billig ble det nok, men brukeren hadde liksom ikke tenkt seg den omveien. Slike overraskelser gjorde brukere flinkere til å beskrive sine behov og preferanser for agenten, men det hendte også at brukerne mente at det var for drøyt, og at de måtte være *ubundet* av avtalen.

Det var nettopp slike eksempler som førte til et krav om at agenter måtte ha et selvstendig, økonomisk ansvar. I og for seg er ikke dette merkeligere enn å gi et aksjeselskap eller en annen juridisk person et slikt ansvar. Det førte til at enhver elektronisk agent måtte ha en grunnkapital i ryggen som agenten selv kunne holdes ansvarlig for. Denne kapitalen er i dag selvsagt ett av de forhold som andre agenter kontrollerer i forhandlingene, det kan nærmest minne om gammeldagse kredittkort som kunne ha ulike kredittgrenser, hvor en høy grense ga brukeren fordeler.

Ved Den internasjonale konvensjonen om elektroniske agenter av 2020 (Bagdad-konvensjonen) ble det skapt et rettslig rammeverk for elektronisk handel med agenter. Og slik fikk Nettet de første «innbyggerne» som befolket det internasjonale og grenseløse kybernetiske landskapet. I dag finnes det mange former for slike autonome, elektroniske enheter med et selvstendig økonomisk ansvar. Men de elektroniske agentene var altså de første, de er så å si Nettets urinnvånere.

THE POLICIES OF LEGAL INFORMATION SERVICES: A PERSPECTIVE OF THREE DECADES[1]

JON BING

1 Introduction[2]

Today, online legal information services are tools of the legal working environment for lawyers in many countries, certainly those in North America and Europe. They are to some extent trivial, and used as a matter of course, which may make us forget that they really have been developed by lawyers still active as researchers, not part of our history, but part of our own times.

2 Europe's problem in 1970: The information crisis of the law

In an important book published in 1970 – *Informationskrise des Rechts und Datenverarbeitung*[3] – Spiros Simitis analysed the current status in Europe. This analysis has a wide scope, but some of the observations were as follows.

During the last decade, European countries had established welfare systems; a change had been made from welfare that rested purely on the appraisal of need, to systems based on rights to social benefits. In these systems, embedded in administrative law, there had emerged certain appeal institutions or tribunals, or established agencies for reviewing administrative deci-

---

1 This paper is based on the contribution to Peter Mirfield and Roger Smith (eds), *Essays for Colin Tapper* (London: LexisNexis Butterworths, 2003), pp 147–158, and the paper "Legal Information Services" for the International Conference on "Law and Computer Science", Havana, 29th September – 3rd October 2003.

2 The historical background is set out in Jon Bing *et al*, *Handbook of Legal Information Retrieval* (Amsterdam: North-Holland, 1984), also available at <http://www.lovdata.no/litt/index.html>.

3 Karlsruhe: Verlag C F Müller, 1970.

sions which had been given increased responsibility. These agencies were not necessarily courts, but were at least similar to courts in the respect that they adhered to the same ideals as a court, and defined their function as guaranteeing "due process", "rule of law" or *Rechtssicherheit.* The legal sources on which these agencies based their decisions, were – also in the Continental European systems – to some extent their own previous decisions; at the very least, they wanted to appear consistent in their application of law. At this time, the number of appeal cases increased rather sharply. As appeals generally were free of charge and part of the administrative procedure, those who felt they had not received the benefits to which they had a right (or a hope), would be inclined to appeal negative decisions. Therefore, a rather high proportion of the negative decisions were appealed. At the same time, the number of decisions increased due to demographic factors. The appeal agencies could not always screen cases (though strategies for this were soon developed), and backlogs mounted. These could only be reduced by two strategies, either by increasing the resources for case processing, or by reducing the resources necessary to process an average case.

Manpower for increasing resources was not forthcoming. Therefore, the alternative was to cut down on the resources necessary to process an average case. As research of the prior decisions of the agency was time-consuming, it appeared as a possible solution to apply computerized systems to make this more efficient.

Looking at the initiatives taken in different European countries, one may see a tendency for agencies or institutions such as those characterized above to be prominent. In Italy, the Corte Suprema di Cassazione took an initiative as early as 1963–64; this was central in establishing the information system Italgiure, which was initially concerned with the dissemination of the *massime* of the court itself to subordinate courts or agencies. In France, an initiative was taken by the Conseil d'état in 1967, the result being the creation of Centre de recherche et développement en informatique juridique (CEDIJ) in 1969, with strong links to the Conseil d'état and administrative courts, but also the Ministry of Justice. In Sweden, the Directorate of court administration (established in 1975) started with the decisions of the administrative courts, and in Finland, the Supreme Administrative Court at the same time took the lead.

These are examples characterizing a trend. Obviously, there are examples of other types of initiatives, but it is maintained that the initiative was typically taken by a national court or other appeal tribunal within the sector of public administration. It may also be argued that the investments typically were justified by claiming they would reduce costs in the legal research associated with an average case, but that the expected economic benefits were not

realized. If challenged, the argument would typically be amended: the better research facilities improved the quality of the decisions, and as the investments should be seen in the perspective of "due process", an economic analysis was inappropriate. The emphasis was thus shifted from a reduction of cost to an increase in quality. One should, perhaps, see this as not only a tactical dodge, but also as reflecting the real concerns of these institutions in meeting the standards set by "due process" for their operation, standards which were derived from those applied to the general courts working under rather different constraints.

An interesting example is Germany. In 1967, the Ministry of Justice started planning a legal information system, the preparatory work resulting in a report for the establishment of Das Juristische Informationssystem[4] (JURIS) in 1972. For the impatient, the plan seemed to take a very long view; it started with a "development phase" in the period 1973–1982. The system was launched within two areas: decisions in social law (based on the Bundessozialgericht) and tax law (based on the decisions of the Bundesfinanzhof). In this way, the plan fits well with the premises indicated above, reacting to the pressures brought to bear on administrative courts.[5] But during the development phase, new databases were continually added.

Also, the only really detailed study of the business economics of such a plan was undertaken for the JURIS system, concluding that for the public sector, an average time reduction of 1.4 hours could be realized, corresponding to 54.60 DEM per week in 1976.[6] Though the study is rather theoretical, and based on presumptions that are hardly valid,[7] the study illustrates how the necessary investment in the legal information service is based on a "rational" and economic argument.

But the plan also contained the concept of an "extended JURIS system", which would be a general national legal information service for all federal legal sources; and the material for the different states (*Länder*) is now being completed.[8]

---

4 *Das Juristische Informationssystem: Analyse, Planung, Vorschläge* (Karlsruhe: Verlag C F Müller, 1972). The Germans chose the same acronym for their service as the US Justice Retrieval and Inquiry System, with the consent of the US Department of Justice. Juris is, by the way, also the name of an Austrian wine and snapps.

5 Note that Professor Spiros Simitis was part of the three-man committee contracted by the Ministry of Justice to suggest the design of a computerized system in 1969 (the two other members being Professors Klug and Fielder).

6 Cf Reinhold S Gluck, *Wirtschaftlichkeit juristischer Informationssysteme* (Darmstadt: S Töche-Mittler Verlag, 1976).

7 Cf Jon Bing, *Rettslige kommunikasjonsprosesser* (Oslo: Scandinavian University Press, 1982), pp 265–266.

8 The home page of JURIS is <http://www.juris.de/produktion/juris/WebSite/juris/juris.htm>.

In JURIS, we have exemplified another major characteristic of the development of the European systems that were initiated in the 1970s. Though their start typically was limited to a certain court or agency within the public sector, and justified by the needs of this institution, their ambition was soon escalating into a vision for an integrated legal information service for the whole jurisdiction. This service would offer case law, statutes and regulations. It would require an effort over time, incrementally building up the databases. But in a few years (and the JURIS example illustrates that we are talking about a decade or more), a general service for professional users of legal sources would be available – a user group often characterized as "lawyers", though it would include professionals and "para-legals" without formal legal education within public administration and private organizations. This is in contrast to a service which would have a more general target group: the public at large or the "layman".

One of the reasons why the vision of the national legal system extended only to professionals was the technological environment. At the time we now are discussing – the end of the 1970s – the information systems were accessed by terminals. These were comparatively expensive, and there were few terminals at a user site. The communication relied often on dial-up lines with a rather low baud-rate for transmission. The user interface was line-oriented, one line was communicated, a new line received – the user could not edit the screen. And communication relied typically on commands in certain formalism. Though attempts generally were made to make such commands easy to understand and remember, they nevertheless were rather cumbersome. Such systems could cater for professionals, but could obviously not be offered for general use.[9]

It may be argued, therefore, that European legal services were poised at the end of the 1970s to grow into general services for the different national jurisdictions. The vision was there, and perhaps also some impatience with users not realising the potential benefits of the systems. The Commission of the European Communities (EC) launched a technical study on the use of the different national legal services,[10] and this reported on the problems of interfaces, lack of availability etc, indicating many of the reasons for the services

---

[9] But at this time, videotex systems emerged, using a television set and a dial-up modem as user interface. Many of these were rather successful, including a couple in the UK, home of the Prestel services (like Infolex or Lawtel). In France, the Minitel was a success, to such a degree that it is argued that it held back the deployment of Internet.

[10] Cf *Technical Study in Legal Information Retrieval,* vols I–III, EC Commission, Brussels, 1977 and *Technical Study in Legal Information Retrieval,* vols I–V, EC Commission, Brussels, 1978.

not taking off in the way predicted by those (the author included) who were looking for general use of such services by professionals.

Then came the unexpected arrival of the personal computer and office automation.

3 The 1980s – the decade of distributed computing

IBM launched its first "personal computer" based on the Intel 8088 microprocessor in 1981, which marked the start of a revolution in office automation. In the context of this paper, it is important to indicate the shift in focus that the introduction of PCs represented. In a surprisingly brief time, typewriters were lifted from the desks in all sorts of offices, leaving a free space where a PC could be placed. These had software that was much more user friendly than that available on the typical terminal linked to a time-share mainframe – one should recognize that even the MS-DOS operating system was comparatively user friendly. But they were very modest in our terms: A typical PC featured a monochrome monitor, 16k of RAM and one 5.25-inch diskette drive (hard drives were not commonplace for another three years).

The change in focus was then from the services available from mainframes through terminals, to the services offered by the PC on the user's own desk. In many respects, this made services more available, one became less dependent on third parties, one got a better and more direct control over the programs and the tasks, etc. Yet in addition to the many advantages, there also was one major disadvantage: PCs were initially stand-alone equipment. Even sharing peripherals like printers, was not trivial. As a consequence, the vision of the integrated national legal information service suffered – such services presumed communication to a common database, and initially PCs simply did not support this.

Speaking in broad terms, one may maintain that the distribution of computing, symbolised by the PC, demolished the vision of users connected to a common legal database. Slowly, PCs were connected in Local Area Networks, and one could – perhaps – see that the foundation was rebuilt for an enhanced situation, where the user did not have to walk up to a terminal in order to link to the computerised legal service but would be able to access that service from his or her own desktop computer. But it took considerable time to realise these new possibilities.

Therefore, solutions were sought for this new situation. In 1980, Phillips and Sony had proposed a standard for a machine-readable compact disk (CD), and, in 1983, prototypes of compact disks for read-only-memory (CD-

ROM) were demonstrated. Compared to the storage capacity of the current magnetic disks, the CD-ROM of 650 MB was impressive. It was also sufficient to offer legal information services. The early CD-ROM of the Norwegian Lovdata foundation offered consolidated statutes in force and all national and local regulations in force on the same platter.[11] This disk could be inserted in a station of the user's own PC, and make the material available in the same environment as the other office tools.

Yet even if the new, compact storage medium had a relatively high capacity, it did not measure up to what was necessary for a national legal information service – again, the requirement to represent the volume of case law easily exceeded what was available on one CD-ROM. There were experiments offering services on several CD-ROMs, but this proved inconvenient – the user had to juggle between the different disks, hyperlinking across disks was awkward, and if the disks were made available on a local area network, the server would have to support several disk stations. Therefore, there was a tendency to define services which could be supported by a single CD-ROM, containing both the retrieval program and the legal data. These tended to be specialised services. There were many business opportunities for such services; the most popular being perhaps services for tax law, but there were many other variations: building and planning law, intellectual property law, EC directives etc. However, these services were more clearly focussed on market segments, and the users within a particular segment had to be able to pay for the service. Therefore, sectors of the law which offered less of a business opportunity would not be covered by the specialised services – for instance, social security law, where the legal aid to clients was mainly offered by agencies within the public sector rather than by lawyers in private practise.

Another feature also made the CD-ROM proposition attractive. CD-ROMs could be marketed as physical objects in the same way as conventional printed books. Therefore, traditional publishers easily could see how their marketing channels and strategies could be adapted to offer this new form of "electronic publishing". For on-line services, these strategies could not be easily adapted.[12]

---

[11] This is a pun: The CD-ROM was using the technology of Silver Platter, which ceased operations in June 2003.

[12] This is not say that some traditional publishers did not take an interest in on-line services. The Thomson group was very active in several countries, and owns today one of the major US services, Westlaw, while the other major service, Lexis, is owned by Reed Elsevier. In this paper, however, the pricing issue will not be pursued as such, though there may be a few notes like the one above.

The retrieval software was also different. In the days of batch processing systems, much emphasis had been placed on the construction of the search request and strategies optimising retrieval performance. When on-line systems came along, making it less of a practical problem to rephrase a request that did not perform as expected, there was somewhat less concern with preparing the request, as users would work more on a trial-and-error basis. Yet still tradition prevailed; the systems often had possibilities for making complex queries, and strategies might include ranking of results. This was especially important for case law, where documents were long and where the search requests often would try to express rather subtle issues of law.[13] The systems of CD-ROMs, however, typically supported rather simple search strategies, often only allowing the user a search request of one term, or a few terms combined by Boolean operators.

One may mention in passing the important distinction between fact retrieval and interest retrieval. In fact retrieval, the user may define the criteria for "relevance".[14] For instance, if a user looks for a book by a certain author, the user expects the name of the author to appear in the field of the document defined as "author's name". If the system gives a negative response, this is interpreted as there not being stored any documents by the specified author. Compare this with a user looking for a case on a certain subject, for instance "liability of the owner of a house when a person is injured by a loose brick falling from a balcony". Obviously, the user could not conclude that if the case did not contain the term "brick", it would not be relevant – if the falling object was a tile from a badly maintained roof, the case concerning this damage may easily be deemed relevant. Lawyers, especially working with case law, need systems to support interest retrieval; the strategies supported by most CD-ROM based systems had been developed for fact retrieval.

Taken together, the CD-ROM based services emphasised the fragmentation encouraged by the nature of the early office automation. The old paradigm had been that of a centre reaching out through telecommunication lines (admittedly often offering communication of low quality), interconnecting all users through a central computer facility from which the services were offered. The new paradigm was that that of a large number of self-sufficient

---

[13] Referring back to the initial experiences of Tapper, we see a connection. The fact that the consistency in indexing was less than satisfactory is perhaps best explained by the indexer seeing different facets of a case in different contexts. Likewise, the legal argument using analogous reasoning may utilize a case of a horse injuring a pedestrian when arguing the liability of the owner leading his or her dog down the street.

[14] This term is in itself an issue, but in the context of this paper, the possible definitions of relevance will not be pursued.

islands. The idea of the integrated national legal information service was perhaps not lost, but certainly downgraded. Computerised legal research became more common, but the services offered were typically specialised or limited in scope.

4 Networking and web services

In the early 1990s, a latent situation had been created by two somewhat different developments. The first was the distribution of computer power sketched above, which had resulted in placing a work station or PC on the desk of most lawyers. At this time, these were also linked together in local area networks.

The second was related to the Internet, a solution for interconnecting computer facilities in universities and research institutions. This had originally been sponsored by the Advanced Research Program Agency (ARPA) of the US Department of Defence, but had around 1980 been split into two separate networks, a military (Milnet) and a civil (Internet). The National Science Foundation operated the latter, and enforced the policy that only research institutions could be linked to the net. The e-mail service supported by Internet became very popular, and was certainly the feature within the network which attracted new institutions and secured its growth. Around 1990, NSF also discontinued its support to Internet, leaving this infrastructure in the hands of the self-regulatory bodies that had grown up in the Internet community, along with the national organisation co-operating with these.[15] As the NSF relaxed its control, other organisations than those charged with research and development, were allowed to connect to the Internet, mainly to get access to the e-mail services. The foundation for a commercialization of the Internet had been laid.

The catalyst exploding the latent situation into a feverish development was the World-Wide Web. The Web was originally conceived and developed by Tim Berner-Lee of the European Organization for Nuclear Research (CERN)[16] in order to facilitate the large, high-energy physics collaborations which demanded instantaneous information sharing between physicists working in different universities and institutes all over the world. Together with Robert Cailliau, Berner-Lee wrote the first WWW client (a browser-

[15] The historical sketch above is rather rough, but in the context of this paper, it is sufficient to make the point.

[16] CERN is an acronym of Conseil Européen pour la Recherche Nucléaire, the official name of the organisation until 1954.

editor running under NeXTStep) and the first WWW server along with most of the communications software, defining URLs, HTTP and HTML.[17] In 1993, Marc Andreessen released the first web browser, Mosaic. At the end of 1993, only fifty servers world-wide could access the Web. This number increased sharply, as the new mass-medium for communication and electronic trade was developed.

The development of office automation had, as has been indicated, the drawback that the importance of communication between users and a central facility had been somewhat downgraded. But as local area networks were hitched onto the Internet, and the Web services became available to the local work station of any user, communication was given priority. Yet the structure of this communication network was very different from what had been common at the end of the 1970s. At that time, one would draw a centralised network around a main hub, linking all users to this facility; this made communication between users possible, but only through the central hub. The Web and Internet was more of a distributed network, any node could communicate to any other node, and it did not have an obvious hierarchical structure. One could, of course, create such within the net – a popular service would attract users, and within the distributed network the service could function like a central facility shared by a large number of users (as the Napster case demonstrated).

One of the fascinations with the new technology was the ease and low cost of establishing home pages, enabling institutions to present themselves and to provide information to the external world. Rather than using the technology to collect information from many sources, presenting them in a co-ordinated and integrated way, a profusion of initiatives was taken – each court, each agency, each institution presented their own site to the public. Initially, therefore, the tendency to fragment was further emphasised. The user, who wanted to search for national sources, was presented with a rather differentiated, if not confused, situation where the different sites might have different standards for updating response, document design, retrieval strategies etc. Moreover, the services offered at Web sites generally adopted the standards for retrieval which are common for search engines, and which support very simple strategies, mainly based on single word or a phrase, occasionally supplemented by simple Boolean operators – and clearly insufficient for the support of interest retrieval.

This new technology created a tension between the older commercial services and the new possibilities. Legal sources like statutes, regulations and

[17] Abbreviations for "Uniform Resource Locator" (the address of a web site), hypertext transfer protocol and hypertext mark-up language (for page definition and description).

decisions, are not subject to copyright in most jurisdictions,[18] and it might be seen as a paradox that the user would have to pay for access to this material. It was tempting to set up alternative services competing with the older.

One of the major examples is provided by Legal Information Institutes. In 1992, the LII of Cornell Law School[19] was launched by Peter Martin and Tom Bruce. "The legal information industry in the US in the mid-'90s had focused totally on judges and lawyers and hadn't paid attention to the information needs of others", Peter Martin has stated. "One of our powerful early discoveries was how much demand outside those professional sectors there was – ordinary citizens trying to make sense of laws that impinge on their lives".[20] The site offers the United States Code, an organized compilation of current federal laws; and the collections of all recent opinions of the US Supreme Court and New York State Court of Appeals. The site also provides topical overviews of such areas as banking law and employment discrimination law and organized collections of links to sites offering court decisions, statutes, regulations and other legal materials. Making information accessible on the web in a manageable format has been a challenge – there are 13 US Circuit Courts, each putting its decisions on the web. The problem is that data structures and formats differ from site to site: researchers need some solution, for instance a search engine that reaches across those structures.

The Cornell Law School LII may have been the first site of its kind on the Web.[21] In the meantime, LII has become a generic term indicating a certain type of operation on the Web,[22] and there are namesakes as far-flung as New Zealand, Zambia and Kazakhstan.

One of the more remarkable LIIs, is the Australasian Legal Information Institute (AustLII), jointly established by the University of New South Wales

---

18 And in most jurisdictions where the state in principle retains copyright to such sources, the exclusive rights are not used to control third party use of this material.

19 See <http://www.law.cornell.edu/>.

20 Quoted in Linda Myers "CU Law institute web site has latest legal information, from Miranda to Elian", <http://www.news.cornell.edu/Chronicle/00/4.27.00/Legal_Info_Inst.html> [25th July 2002].

21 One will appreciate that 1992 is very early indeed for such a service.

22 The term "Legal Information Institute" (LII) refers to a provider of legal information which is independent of government and provides free access on a non-profit basis to multiple sources of essential legal information. See further Graham Greenleaf, Philip Chung and Andrew Mowbray, "Free access to law via Internet as a condition of the rule of law in Asian societies: HKLII and WorldLII", <http://www2.austlii.edu.au/~graham/publications/2002/HKLII_WorldLII_Jan02/HKLII_WorldLII.html#Heading3> [25th July 2002].

and the University of Technology, Sydney with Graham Greenleaf and Andrew Mowbray as initiators. This is an effort with an impressive ambition and a background in the policies of legal information services in Australia, where the doctrine of "Crown Copyright" prevails. AustLII argued that unless governments and agencies positively co-operate with non-commercial bodies which wish to provide information via the Internet by providing them with raw data in computerised form, non-commercial bodies are unlikely ever to be able to publish the data in any form.[23] There are several characteristics of the AustLII that make the service remarkable – the scope of the database is one thing, the programs developed to enhance the service, and support search strategies are another. But perhaps most important are the standards AustLII sets itself for making legal sources available in a complete and authentic form, a service to integrate material and to be trusted.[24]

AustLII has also many offspring, one of them being the WorldLII, a co-operation between itself and the British and Irish Legal Information Institute (BAILII), Canadian Legal Information Institute (CanLII), Hong Kong Legal Information Institute (HKLII), Pacific Islands Legal Information Institute (PacLII). It also includes databases provided by Wits Law School, South Africa. It is an attempt to create a truly international information resource; not only are the materials made available by the LIIs listed, but a search engine has been developed to index legal sites around the world.

The story of the LIIs has still to be written, and this paper can hardly do more than indicate the important policy implications of this movement. But some tentative issues can be discerned.

First, the initiatives are typically associated with universities and law schools. This is by no means the first time policies have sprung from this source. The first documentation centre to emerge in France was the Institut de recherches et d'études pour le traitement de l'information juridique (IRETIJ), the result of an initiative taken in 1965 by Professor Pierre Catala at the University of Montpellier. The main focus of this institute was initially on the decisions of the 32 French appeal courts, which were not subject to systematic publication.[25] This was a problem that researchers at several universities set out to address, though IRETIJ remained one of the few centres to pursue this policy throughout the 1970s.

---

[23] Graham Greenleaf, Andrew Mowbray, Geoffrey King and Peter van Dijk, "Public access to law via internet: the Australasian Legal Information Institute", <http://www.austlii.edu.au/austlii/articles/libs_paper.html#RTFToC11> [25th July 2002].

[24] Also other LIIs have similar standards; for Cornell LII, see Thomas R Bruce, "Some Thoughts on the Constitution of Public Legal Information Providers", <http://www4.law.cornell.edu/working-papers/open/bruce/warwick.html> [25th July 2002].

[25] There existed only two reporters, one for the Paris and one for the Grenoble appeal courts.

Second, there is indication of a tension with respect to the objectives of the services of the LII. As stated by Peter Martin and Tom Bruce (the co-directors of Cornell LII), legal information services were mainly concerned with the needs of the professional user of legal sources, perhaps even limited to those with a formal legal education. The ideal of *publicatio legis* requires that the law is available to all, and this certainly can be perceived as a necessary foundation of a democratic state. Therefore, the limited publishing through specialised services may be seen as too restrictive to provide the necessary legal information for the citizens of a modern state. In the last part of the 19th century, many jurisdictions changed their system of communicating statutes and other important legal instruments to the public, adopting some form of printed gazette to replace, typically, the public reading of texts from the steps of the church. It would seem appropriate that given the possibilities of new information technology, these were exploited to give the public better access to the law.

Indeed, this has happened in many jurisdictions. France is from 15th September 2002 reforming its legal information services from the commercial service, Jurifrance,[26] to the free service, Legifrance. From 1st January 2001, Norway changed its principle for the official publication of statutes, regulations etc from the printed version (*Norsk Lovtidend*) to the Web publishing of Lovdata. The printed gazette is still published, but is no longer the official publication. The former system made the official printed version available to a few thousand subscribers; the new system reaches, through the Web, potentially all of the approximately two thirds of Norwegian households that have access to Internet.

Yet one should not mistake the policy of *publicatio legis* with the needs of the professional user of legal sources for an efficient research tool. The public certainly should be given as easy access as possible to statutes and other important legal instruments. But use of the authentic legal sources is certainly not trivial. The public should ideally have a problem-oriented gateway to the material, where the authentic instruments are commented and explained. This is often done within specialised areas where there is a perceived need for legal aid, typically by public agencies through guides, popular presentations etc, and by doing this on the web, the legal sources may be presented hyperlinked into a rich environment of material. But this strategy requires resources for presenting the law and keeping the presentation current – there are, to the author's knowledge, no examples of such a service covering the whole area of law. If all authentic sources – statutes, regulations, court deci-

[26] See <http://www.jurifrance.com/> [26th July 2002].

sions etc – were made available, this obviously cannot satisfy the needs of the lay user.

The services offered by the LIIs are often buffered by the policy of *publicatio legis* and a reference to the basic right of all citizens to know the law. This justification is *not* challenged here. What is challenged is the presumption that it is wise, or even possible, to satisfy *both* the needs of the lay user *and* the needs of the professional user by the same information service. Even though much of the authentic material would be identical, the user requirements for a friendly service would differ. Possibilities for sophisticated search requests would not necessarily be helpful to a user only occasionally using the system; the semantics of hyperlinks would at least have to be explained, the principles for interpretation of decisions from the different courts, the harmonisation of the results both when decisions were not consistent, and with respect to statutory rules with different application in time, would be complex and not at all easy, even for an experienced lawyer.

The tension between these two objectives can be discerned in several aspects of services from LIIs. For instance, Cornell LII integrates it services with legal education, and AustLII has several features to help lay users.[27]

5 From retrieval to regulatory management

The discussion of the historical development above demonstrates how legal information services have been conceived as *retrieval tools,* helping the professional lawyer – and perhaps even the well-oriented layman – to conduct legal research. In one sense, this is a restricted view, leaving out other activities in which the legal instruments are important, especially regulatory management – ie, preparation, drafting, adopting and reviewing statutes and regulations. In this chapter, the perspective will be changed. It is suggested that this may be proper for a country which is not – like the North-American or European jurisdictions – seeped in traditions and established arrangements, where the new computerised service has to find its place among legal publishers of primary and secondary sources, legal gazettes, and other well-established practises.

The author has a modest experience with the challenges of developing countries.[28] There are many considerations which have to be made in a coun-

[27] One of the innovative features of AustLII is an expert system integrated in the information service. When the user has identified a provision in a statute, the user may (where available) switch to an expert system mode that will guide the user through a series of questions in order to advise the user whether the provision will apply to the problem of the user.

try where resources are scarce, and where the technological infrastructure, including telecommunications, may not be reliable. The institutions and professionals working within the jurisdiction that the author has encountered, have impressed upon him the importance of their expertise and efforts to realize the objectives of the legal system in question, particularly in a situation where resources elsewhere taken for granted – like a sufficient stock of paper, office (floor) space, etc – are lacking.

One of the lessons is that one should design a system to cater simultaneously for several levels of technology. Within the central administration, there may be available a high-speed telecommunication network linking workstations of users, while in other districts one cannot rely on land telecommunication links, and will have to rely on systems catering for standalone workstations or for traditional paper publications.

Another lesson is that one should design an *integrated* system which caters for the bureaucracy, the legislator, and the legal profession.

There is hardly any example of such a system in existence, but it is sketched here for discussion and consideration.

To describe the system, we start with the establishment of a database. This will contain the major legal sources. What these major legal sources are exactly, will obviously depend on the law of the land, which will qualify what is necessary or important when making a legal argument. It will include the statutes adopted by the parliament and the secondary regulations issued by authority of the statutes (or the constitution) by the government. There will be variations, these should be defined by the constitution, and may be of a variety baffling to a lawyer not used to the traditions of a foreign jurisdiction. In this discussion, we will gloss over this possible complexity by presuming that there are only two types of regulatory instruments: statutes and secondary legislation (both of which will be included in the term regulation).

To establish the regulatory database, one first has to establish a group of editors. This is independent of the technology used for the system – any system has to have competent editors to make informed choices in maintaining the database. This point need to be emphasised, and is one of the major causes for such a system to be centralized. This is not a function of technology (which may permit a distributed system) but of exercising the necessary editorial control to secure the high data quality necessary for a regulatory management and legal information system.

We also presume that material will be available from the courts, if the legal system makes case law a relevant source (which is generally the case, at

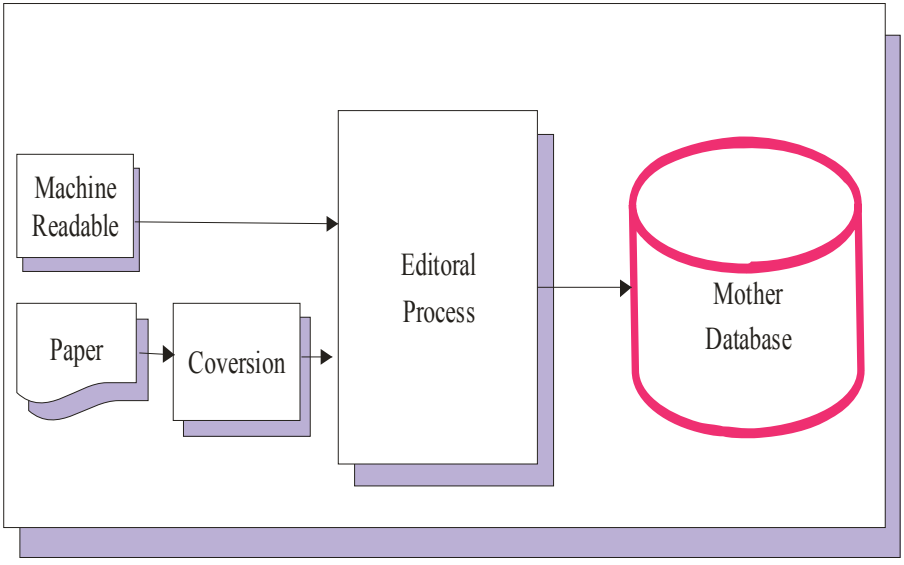
---

[28] These include Tanzania, Bulgaria, the Baltic republics and the jurisdictions of former Yugoslavia.

least regarding decisions from the Supreme Court, Constitutional Court or other important courts). If the jurisdiction adheres to the common law principles, decisions by lower courts may also be important. The regular publication of case law will often be a practical problem, and we want our integrated system to contribute towards a solution. Such decisions may be available in computerised form, but may also have to be converted by the editors.

In establishing such a system, one has to pay respect to many trivial matters. One of them is how the material is made available to the editors. We presume that regulations are made available in machine-readable form. But the editors will have to convert that form into a standard format to be used on the system. Several considerations have to be made. The most important would be to make sure that the material is marked-up, typically using SGML.[29] Another important activity would be to *normalise* certain elements, especially dates and citations. This will be important for creating and maintaining hyper-links in the database produced for legal research.

Thus, we have the first stage of the system: the creation of a "mother database" in marked-up format and with normalised elements:



[29] Standard Generalized Mark-Up Language, see <http://xml.coverpages.org/sgml.html> or Jon Bing, "Copymarks: A Suggestion for Simple Management of Copyrighted Material", in Jon Bing and Giovanni Sartor (eds), *The Law of Electronic Agents,* CompLex 4/03 (Oslo: UniPub, 2003), pp 198–201.

The important point is that the mother database is not an end product but a production platform from which other products may be created. The material is here marked-up with explicit meta-information. This implies that one may use the mark-up to associate different functions with the definitions. There may be a mark-up insert defining a line of text as "heading, statutes". If we want to print the statute, we will associate the definition with the instruction, "Start on top of new page, centre, Times New Roman pt 16, bold, black". If, however, we are updating a retrieval database, we may want to give a different definition, such as "Start of new document, retain text line, insert in each subsequent paragraph as first heading, display as Veranda, 14 pt, aligned left." This will copy the title into the paragraphs of the instruments, and when retrieving a paragraph, the user will be able to determine of which instrument the provision is a part. One will appreciate that a systematic and conscious use of the mark-up language will retain information of the "semantics" of the elements in the text, though this "semantic" is limited to identify the role which the identified element has in the text. Associating different applications to the marked-up document, the meta-information may be interpreted in different ways, making the mother database part of a flexible and powerful "engine" driving the different elements of the integrated legal information systems.

One of these elements may be the *legal gazette.* It is customary that the official publication of new legal instruments is done by a dedicated publication. Often the publication is a requirement for the regulation to take effect, making this a vital element in the legal information system.

This principle is often known as *Lex Gambetta,* named after a French minister who introduced the system. Historically, the publication of an official, printed gazette typically replaced the publication through a public reading by official heralds, or by priest reading the regulations from the steps of the church. As the publication often is necessary for regulations to take effect, many jurisdictions have introduced measures to ensure that the publication is not made difficult or impossible by a strike among the printers. In some jurisdictions, the legal gazette is integrated with other functions of publishing certain types of notices or declarations, like the liquidation of companies, public tenders, etc. One may want to consider organising the gazette in such a way that the regulations are published separately from other notices.

As a regulation in some jurisdictions is not deemed public before published in this way, a government printing office is created. In the suggested system, this function is absorbed by the integrated legal information system, but the tradition of a government printing office has proved in some cases to be an obstacle to the development of such a solution. This may also be one of

the organisational features to be addressed when developing an integrated legal information service.

By publishing the legal gazette from the mother database, the text becomes available at a very early stage for the integrated legal information service, and may be used also for other purposes.

One such other use will be the *database for retrieval.* We suggest that the database should be a *status* database, which implies that it at all times reflect the law as it is. Adopted instruments not taking effect, may be represented in the database. As they take effect, a consolidation will take place under the guidance of the editors, and the amending instruments will be consumed by the instruments they are amending, with the exception of provisions that cannot be consolidated – typically transition rules. The repealed instruments are not deleted, but made available by an auxiliary function.[30]

This point may need some elaboration. A major activity of regulatory management is to amend regulations, to make them meet the changing needs of society and the dynamic legal context in which they are embedded. Different legislative principles of amendment may be applied.

One is the *principle of textual replacement*, which requires that any amending instruments exactly identify which provisions are amended, and specifies what text will be replacing the identified provisions. In this way, one should be able, in principle, to "cut-and-paste" from the amending instrument to the identified provisions in the amended instruments. This principle makes it rather easy for the editors to consolidate the existing body of regulations.

An alternative is the *principle of omnibus replacemen*. Under this principle, the amending regulation has a general clause specifying that any provision in previously adopted regulations which is in conflict or differs from the amending regulation, is repealed – without identifying which provisions that will be amended in this way. This principle – which is applied in many jurisdictions – makes consolidations difficult to produce. Any lawyer will appreciate the difficulty which will arise in deciding whether two provisions really are in conflict, or if they, eg, may co-exist because they govern slightly different situations.

---

[30] Methods for solving the problem of historical material are rather complex. The problem may be solved using sophisticated programs that retain information on the time in which each element of the regulation has been in force, using "current" as default. A more simple solution would be to document the repealed sections in a historical database, but hyperlink them to the current provisions for easy access.

Therefore, the basic rules of regulatory management with respect to amending regulations may be something to consider when deciding to create the integrated system suggested in this paper.

The database will be offered on-line for professional users. A number of policy issues will have to be resolved in offering this service – the retrieval software (which should be efficient, cater for interest retrieval, and have a user-friendly interface), the tariff structure (whether the users should pay, and if payment is chosen, the way in which remuneration is calculated) and a number of other principles.

In order to be successful, there are two guiding principles relating to the database as such. First, its *coverage* should be as large as possible. If the users cannot trust to find the material in the database, they will be reluctant to use the service. Hence, the historical back-log has to be computerised and integrated in order to ensure sufficient coverage; this itself may require a large investment. Secondly, the *updating response* should be as short as possible; this is the time from when a change is made to the regulations until the change is reflected in the database. Ideally, the updating response should be zero, something which is possible if the legal gazette is integrated in the overall legal information service.

A major point made above is that some countries cannot rely on a computerised legal service due to a lack of sufficient infrastructure, or distribution of computerised solutions among all end-users. Most jurisdictions, therefore, in addition will print a *compilation of statutes in force* (and compilations of regulations, if deemed desirable). This compilation will be a paper version of the regulatory database, and may be reeled off from the mother database in the same way as the computerised database, only interpreting the meta-data in a different way to produce the necessary codes for governing the printing process. Using this technology, such a compilation may be produced regularly by certain intervals – eg, annually or bi-annually. The printed version will be voluminous, and the challenge of printing, binding, stocking and distributing such a publication will itself be considerable. There may be occasion for the legal information service to seek co-operation with a publisher with experience in handling such a process, including the distribution through book-stores or otherwise.

Obviously, one may also produce CD-ROMs in the same manner, including an appropriate retrieval system for the compact disk (or disks), which then can be distributed and run off a drive on the workstations of end-users (or be copied down to their hard disk). Numerous other products may also be made available on request, for instance specialised compilations for certain areas of law, or for certain internal jurisdictions.

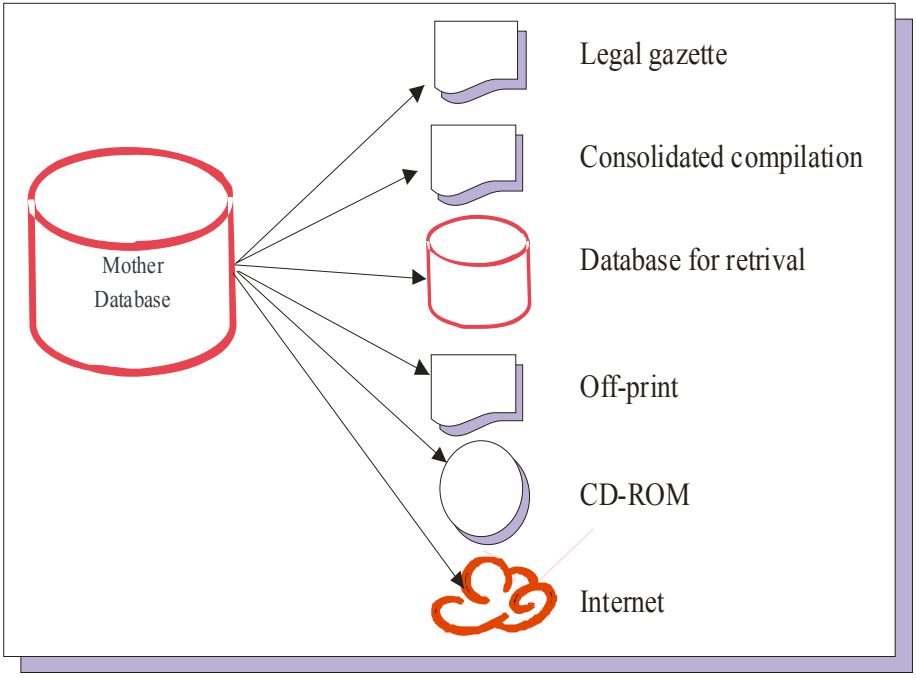
The legal information service should not be a monopoly in the strictest sense. Therefore, if a publisher wants to integrate regulatory texts in a book or to publish a selection of such instruments, the legal information service should make the material available in machine-readable form to the specifications of the publisher, but for a fee. This fee would be lower than the costs of the publisher re-entering the text for the publication.

The legal information service should also be charged with making the regulations available on the Internet, preferably free of charge. In this way, all agencies or organisations which need to cite the regulation as part of describing their own services or objectives, would be able to hyperlink to the material, ensuring that it is correct and current at all times. This would avoid confusion, at the same time as the agencies/organizations would draw benefits from the ease of presenting material on the Internet.

What is stated here for regulatory databases also holds for case law. It may be advantageous to have the cases available within the same framework, as it would make much easier hyperlinking from a regulation to a case in which that regulation is interpreted or from a case to the regulation being cited.

As citations are normalised at the time of input, one may have programs which automatically set up the hyperlinks and maintain them for each update of the database. When this is done automatically, there will be marginal effort related to maintaining even a large structure of hyperlinks.

Taken together, this would create a number of different services and publications based on the mother database:



One will note that this solution meets many of the requirements set out initially. It caters for different levels of technology; the system becomes an "engine" which drives the different elements of the information system. Relative to the composition of the user group, emphasis can be put on the delivery system most in demand.

Many may question whether a "database for retrieval" is viable alongside free Internet access to the regulatory information. This has been addressed to some extent above in the discussion of LIIs but will obviously have to be decided on the basis of the characteristics of the jurisdiction in question. There are examples of a database for retrieval catering viably for professional users alongside a free Internet version.[31] In these cases, the database is a commercial system having a higher level of functionality, access to a wider range of documents and services than the free Internet solution, which mainly meets two requirements: the lay-person's need to consult the law of the land (the principle of *publicatio legis),* and the need to have a stable and quality-ensured reference for other websites citing regulations.

[31] At least in France and Norway.

The above solution is not the end of the story when considering the system as a part of regulatory management.

The persons within the government and legislature responsible for maintaining regulations will use the system for several purposes. If a regulation is to be amended, the user will download the regulation as a basis for making the amendments, from the mother database in marked-up format. In this way, the user may utilise the mark-up language and have the proposal reproduced in the forms relevant for adopting an amendment (before the cabinet, the parliament etc), and the adopted and amended regulation will be communicated to the editors of the integrated legal information service in a form which makes it easer to integrate the amended regulation in the mother database.

Further, the retrieval system will support such users when working on amendments or new regulations. One may find other regulations using defined terms, citing the regulation under consideration etc, and supporting the principle of textual replacement.

In this way, the integrated legal information service will support three different user groups with needs that are not fully identical:

- Lay users, who need to consult the regulation in order to determine their own legal position.
- Professional users of legal sources, typically private practising lawyers and civil servants working with legal cases and problems.
- Regulatory managers, working with developing new regulations and amending the regulations in force.

Setting up such a system is also a question of *organisation*, as indicated above. One will appreciate that the system becomes a meeting place for the three main arms of a state – the legislature (parliament), the government (the executive branch) and the judicature (the courts). This may make the location of the organisation operating the system within any of these branches considered less than appropriate – it may be seen as incompatible with the independence of any of the branches with respect to the others. For instance, the government will be party to many legal disputes, and one should be careful to organise the system in such a way as to deflect the suspicion that influence over the legal system, for instance, is used to exercise control of the selection of case law material favourable to the government.

A solution may be to create a *foundation* to operate the system. The form to be chosen would obviously depend upon the law of organisations within the jurisdiction concerned, but there will often be available a form of legal person with limited liability (like a shareholding company) but without owners. Ideally, the foundation would "own itself", like a trust or an "associa-

tion sans but commercial" or the like. This has the advantage that the organisation cannot be purchased by hostile actors in the market.

Such an organisation could be governed by a board composed of representatives of the branches involved – eg, a representative for the government (the Office of the Prime Minister, Council of Ministers, Ministry of Justice or what may be deemed appropriate), the Parliament (the executive director of its administration, chief draftsman or what may be deemed appropriate),[32] and a representative of the judges (perhaps named by an association of judges, the Supreme Court or what may be deemed appropriate). Additionally, it might be desirable to have a representative of the Bar, and perhaps also a representative of academic lawyers. In this way, one has ensured, to some extent, that the organisation would pursue the objectives of the legal system rather than purely commercial and/or political objectives. The board would become a forum for policy decisions on the legal information service of the land among representatives of the branches constituting the legal system itself.

It is admitted that this sketch does not cover all issues. Numerous aspects of both practical and principal nature are not addressed. The objective has been rather limited: to indicate a strategy for the development of an integrated, national legal information service which does not presume a certain technological infrastructure, and which may grow and adapt to the changing social and technological context.

[32] Involvement of the members of the parliament would probably not be appropriate.

THE MEANING OF "DATA" – A LEGAL ISSUE OF GROWING IMPORTANCE[1]

LEE A. BYGRAVE

In broad terms, this essay concerns the relationship of law with information concepts, such as "data". The basic contention of the essay is that important aspects of this relationship need revisiting. Moreover, some of the reigning assumptions about the relationship need revising.

Back in the 1970s and early 1980s, there occurred a great deal of thinking and writing – at least in academic circles – about the interrelationship of law and information concepts. Amongst important contributors to this discussion were Jon Bing, Herbert Burkert, Peter Seipel, Egbert Dommering and Graham Greenleaf. This is not to suggest that these writers (or others) have subsequently ceased to think and write about that relationship. Still, back in the 1970s and early 80s, there seemed to be an intensity – indeed exuberance – of discussion about that relationship, a discussion which waned significantly thereafter. The 1970s and early 80s were heady days: heady in one sense because much abstract, theoretical analysis informed the discussion concerned; heady in another sense because a new and exciting field of legal science was emerging.

It might be said – somewhat unfavourably – that some of the discussion was basically a naming game the endpoint of which was to find an appropriate nomenclature for an emergent legal discipline ("computer law"? "legal informatics"? "information law?"). Yet most of the discussion was essentially seeking to explicate, in a systematic fashion, how the law regulates the processing and flow of information. Within that enterprise, a basic question was: how does the law itself conceptualise information? Concomitantly, what sort of information concepts are utilised by legal rules?

One of the basic conclusions of the discussion was that legal rules – at that time anyway – tended generally to avoid expressly using concepts like "information" and "data"; instead, these items tended to be regulated in more indirect ways, for instance by focusing on certain *media* (eg, paper) or

[1] This essay is based on a speech given at the Columbanus Symposium on "Database Protection and Freedom of Speech", University of Oslo, 30th August 2003. For further details on the Columbanus Symposium series, see <http://www.columbanus.org/>.

certain *structures* (eg, data files) or certain *contexts* for communication (eg, contract). Another basic conclusion was that the legal community had often vague and somewhat inconsistent views of information concepts. This conceptual laxity was contrasted with the more rigorous and systematic explication of information concepts in the fields of informatics and computer science. In those fields, the concept of "data" usually refers to signs, patterns, characters or symbols which potentially represent some thing (a process or object) from the "real world" and, through this representation, may communicate information about that thing. The "information" as such denotes the semantic content of the data.

This way of defining "data" and "information" seems to be in harmony with their conceptual roots. Etymologically, "data" is the plural form for the Latin word "datum", which roughly means "gift". The word "information" stems from the Latin term "informatio (-onis)", which means "representation" or "sketch".

A conceptual framework in line with the computer scientist's view of "data" and "information", together with their etymology, also seems to have found favour – in theory at least – with the bulk of legal scholars who contributed to the early discussion on the interrelationship of law and information concepts. Some of these scholars frequently pointed out, though, that maintaining a division between the notions of "data" and "information" was artificial and unnecessarily pedantic in most legal contexts, as such a division was usually difficult to maintain in practice. Further, the division usually had no significance for application of the law.

Partly as a consequence of this pragmatic standpoint, few serious attempts were made to push the rest of the legal world into more conscious reflection on the meaning and scope of information concepts. Pragmatics trumped theoretical rigour. If we look around at legal policy making over the last couple of decades it is, indeed, marked by a paucity of such reflection and rigour. This state of affairs is all very well if the meaning and scope of information concepts have no practical significance in a regulatory context. Do they have such significance? A couple of decades ago, it was easy to answer "no". Today, however, it is easier to answer "yes".

What is behind this change? In the 1980s, the computer was heralded as liberating information from its then traditionally paper medium. A popular phrase of the time was "the computer has set information free". However, from then on, legal processes have also had a liberating effect. Legal rules are increasingly being drafted in ways that essentially separate information from specified and relatively specific media with fixed physical and logical "walls" – eg, "document", "register", "file". This development is partly in answer to the technological development just mentioned – the liberating of information

from paper-based media. Two regulatory principles – indeed, imperatives – are at play. One is "functional equivalence" (ie, what is legally possible using non-electronic means should also be legally possible using electronic means – thus, eg, digital signatures should have the status of handwritten signatures). The other is "technological neutrality" (ie, legal rules should be drafted so that their application is not exclusively tied to a particular technological platform – thus, eg, new legal rules focus on "electronic communication" instead of "telecommunication"). Steered by these principles, policy makers are overhauling legislation to weed out the formulations of yesteryear and replace them with broader concepts designating a generic function – eg, "communication", "transaction", "information, "data".

A problem with this development is that many of these concepts in the legislative newspeak are complex, vague and open to a profusion of definitions. Concomitantly, their boundaries are nebulous. Legislators and other policy makers do not seem to have paid sufficient attention to this conceptual instability. This inattention is likely to have unintended, if not unfortunate, regulatory consequences.

In Norway, these consequences were first manifested in a case arising within the field of criminal law. In the late 1980s, the Norwegian Penal Code (*almindelig borgerlig straffelov 22. mai 1902 nr 10*) was amended to enable it to better capture aspects of computer crime. Amongst these amendments, a provision was added making it a criminal offence to gain unauthorised access to encrypted "data" stored or transmitted electronically (§ 145(2)). In the case concerned, the Norwegian Supreme Court was called upon to determine whether such an offence was occasioned by the use of so-called "pirate decoders" to receive and decode television signals sent by satellite. The majority of the court interpreted the term "data" as not covering television signals.[2] This was despite the apparent wish of the legislator that the term be given a broad meaning. The preparatory works, though, give otherwise little clear guidance on the intended ambit of the term.

The legal propriety of the court's view of "data" is not of primary concern here. Of greater importance is that the judges took a view of "data" which is not in line with what most information scientists would take. Thus, the case shows that we cannot take for granted that jurists will construe "data" according to the logic of information and computer science. Concomitantly, we cannot expect uniformity of views about the meaning of the

---

[2] *Norsk Retstidende* (Rt) 1994, p 1610 *et seq*. A similar view was taken by the Supreme Court in a subsequent judgment: Rt 1995, p 35 *et seq*. Use of pirate decoders was subsequently prohibited through inserting in the Penal Code a new § 262 – a provision which, somewhat paradoxically, is much less technology-neutral than § 145(2).

concept. The same holds true for many other basic information concepts. Such concepts tend to have multiple definitions each of which has its own claim to legitimacy in a particular context or field. This definitional multiplicity requires that legal policy makers address more rigorously what these concepts are to mean in a regulatory context.

Data protection law provides the next case highlighting this need. Again, the case is from Norway although the issue it throws up is also being discussed elsewhere. The issue is whether the concepts of "personal data" or "personal information" in data protection legislation may extend to human biological material as such (ie, independent of any information that otherwise can be derived from the material). In other words, can blood, sperm, saliva etc constitute personal data or information for the purposes of data protection law? The issue is difficult to resolve on the basis of the legislation itself or the relevant preparatory works. Certainly, when drawing up data protection law, legislators have often intended that the concepts in question should have a wide ambit. Yet they have otherwise tended to take for granted the meaning of the terms "data" and "information", focusing instead on the necessary criteria for linking data or information to an individual person. The terms have otherwise rarely been analysed systematically in academic discourse in the field.

In the case concerned, the Norwegian Data Inspectorate (Datatilsynet) held that blood samples collected and stored for medical research purposes may be "personal information" ("personopplysninger") as defined in Norway's Personal Data Act of 2000 (*lov om behandling av personopplysninger 14. april 2000 nr 31*). The Inspectorate reasoned, in effect, that it was artificial to distinguish between the medium and the message, particularly in light of technological developments. It will be readily seen, though, that the Inspectorate's holding sits uneasily with the conceptual platform common in information and computer science. If one sees "data" as essentially a *representation* of real world objects (or processes), and "information" as a cognitive process involving *comprehension* of the representation, it is difficult to view the human body itself (or parts therof) as data or information. Indeed, this difficulty explains partly why, on appeal, a majority of the Data Protection Tribunal (Personvernnemnda) concluded differently to the Inspectorate on this point.[3] However, one can also read into the majority decision a concern to prevent the scope of the legislation, and thereby the scope of the Inspectorate's area of competence, from being radically extended in a way not originally intended by

[3] See appeal decision in case 8/2002, available at <http://www.personvernnemnda.no/klagesaker/nrVIII2002.html>.

Parliament, without the latter first being given the opportunity to discuss the issue at hand.

A third context which arguably highlights the need for regulators to systematically address the meaning and scope of information concepts, is the legal protection of databases. A discussion is emerging over the precise ambit of the database concept, in particular whether the concept as employed in the European Directive 96/9/EC on database protection, may extend to biobanks, seedbanks and other similar collections of physical/biological material. The discussion is partly ignited by the reference in the Directive's definition of "database" to the ambiguous phrase "data or other materials" (Article 1(2)). How *material* are "materials"? Are "materials" to be limited to the *immaterial*? Once again, the legislation and its preparatory works provide little guidance for resolving these questions.

It appears that no litigation has yet been initiated in which these questions come to a head. Such litigation could be a long way off. After all, who (apart from the occasional academic commentator) is going to bring a court action pushing the view that a database covers collections of physical objects *per se*? There do not exist database protection agencies equivalent to privacy and data protection commissioners. And those who invest in biobanks and the like, and who find it necessary to protect their investments through litigation, will probably sue under other heads of action (eg, larceny, trespass, undue enrichment) than breach of sui generis legislation on database protection. These observations may detract from the *practical* significance of the questions concerned. Nevertheless, the questions remain important in principle and in the broader regulatory context.

It is remarked above that legal processes (in addition to information technology) are having a liberating effect on information. This liberating process, however, runs two ways: at the same time as the law is setting information free, information is, in a sense, setting law free. At the same time as information concepts, freed from any legislative references to specific media, spill over old boundaries, so too does the legislation employing these concepts. While this engenders greater legislative flexibility, it can come at the price of regulatory overreaching. By "regulatory overreaching" is meant not just that the law attains an ambit beyond the conscious contemplation of the law makers but that its ambit is otherwise counterproductive. The law floods rather than irrigates. Or it spreads itself so thinly that its practical effect evaporates. The latter process risks being brought on when, for example, the concepts employed in legislation are stretched beyond their natural or logical limits. All regulators ought increasingly to bear these points in mind when they consider the limits of "data" and other information concepts.

A well-known aphorism from the fields of informatics and systems development is: "garbage in equals garbage out". The expression is intended to press home the point that the extent to which data that are extracted from an information system can be interpreted and applied in a desired manner – in other words, the extent to which the data are not "noise" or nonsense – depends largely on the extent to which they were afflicted by error when they were first fed into the information system. If data are garbage when they went in, they are likely to be garbage when they come out.

It will be readily apparent that there exists a certain parallel in respect to the main issue at hand. If legal policy makers have a muddled grasp of a concept like "data" when they insert it into legislation, the implementation of the legislation is likely to end up muddled too.

CASE-NOTE: JURISDICTION PURSUANT TO THE LUGANO CONVENTION ARTICLE 5.3 WITH RESPECT TO DEFAMATORY STATEMENTS IN TV BROADCASTING[1]

GEORG PHILIP KROG

1 Introduction

The purpose of this article is to present and review a recent decision by the Norwegian Supreme Court concerning the Lugano Convention Article 5.3 in light of the case law of the European Court of Justice (ECJ) concerning the Brussels Convention Article 5.3.[2] The decision (*Norsk Høyesterett (kjennelse)*) is dated 17th October 2001 and was published in Rt 2001, p 1322 *et seq.*[3]

Jurisdiction in international civil and commercial matters within the territory of the European Union (EU) and European Free Trade Association (EFTA) is exhaustively (except for clearly defined matters) regulated respectively by the Brussels Convention of 27th September 1968 and the Council Regulation (EC) No 44/2001 of 22nd December 2001 (hereinafter named the Brussels Jurisdiction Regulation), which entered into force on 1st March 2002, and the Lugano Convention of 16th September 1988.

The legal issue in question was whether or not Norwegian courts according to the Lugano Convention Article 5.3 were competent to adjudicate a cross border dispute concerning the question of liability for allegedly defamatory statements in a TV-program broadcasted from Sweden on Swedish Television with recipients in Norway. The Norwegian Supreme Court ruled that Norwegian courts were competent to adjudicate the subject matter since the place of the harmful event is Norway where the harmful effects occurred.

---

1 A slightly different version of this article is published in IPRax, Heft 1/2004.

2 The European Court of Justice gives authoritative interpretations when solving questions pursuant to the Brussels Convention of 27th September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters according to the Protocol (with joint declaration) on the interpretation of the Convention by the Court of Justice.

3 The case can be retrieved at <http://websir.lovdata.no/cgi-lex/wifthen?Rt-2001-1322>.

For the courts, the functionality and significant value of the jurisdictional rules is to delimit and localize the legal relationship in the sphere of a jurisdiction and determine the attribution of competence to court to adjudicate the subject matter in international civil and commercial matters by as far as possible a unitary application of the jurisdictional rules, subsequently excluding all other potentially competent courts other than the one designated.

For the disputing parties, the purpose of the jurisdictional rules is to create predictability of the applicable law in international matters, thereby enabling the parties to clarify their respective rights, obligations and responsibilities.

When presenting and reviewing the Norwegian Supreme Court case in light of the case law of the ECJ pursuant to the Brussels Convention Article 5.3, one must have in mind that Protocol 2 to the Lugano Convention on the uniform interpretation of the Convention states in the Preamble that the contracting parties' courts are independent in their interpretation and application of the provisions of the Lugano Convention. This implies that the Norwegian Supreme Court does not necessarily have to apply the same methodology as the ECJ, which has practiced as a main rule that the Brussels Convention must be interpreted autonomously. This means that the concepts must be given an interpretation according to the Convention and independent of how the concepts are interpreted in domestic law. Consequently, the ECJ has stated that the provisions in the Brussels Convention must be understood "by reference, first, to the objectives and scheme of the Convention and, secondly, to the general principles which stem from the corpus of the national legal systems".[4]

All terms contained in Article 5.3 must, according to the ECJ, be interpreted autonomously. The notion "tort, delict and quasi-delict" shall be interpreted autonomously and must be regarded as an independent concept covering all actions which seek to establish the liability of a defendant and which are not related to "contract" within the meaning of Article 5.1.[5] Until the *Marinari* case, the ECJ implicitly decided that the term "the place where the harmful event occurred or may occur" bore an independent meaning in the Convention. However, in the *Marinari* case the ECJ explicitly made a principle judgment as ot whether the notion "the place where the harmful event occurred or may occur" also could be interpreted as a reference to the

---

4 *Lufttransportunternehmen GmbH & Co KG v Eurocontrol*, Case 29/76, ECR 1976, p 1541, paragraph 3.

5 *Athanasios Kalfelis v Bankhaus Schröder, Munchmeyer, Hengst & Co*, Case 189/87, ECR 1988, p 1565.

choice of law rules in the forum country.[6] The ECJ rejected this view noting that "the Convention did not intend to link the rules on territorial jurisdiction with national provisions concerning the conditions under which non-contractual civil liability is incurred" (paragraph 18).

However, Protocol 2 to the Lugano Convention was designed to prevent divergent interpretations and to arrive at as uniform an interpretation as possible of the provisions of the Lugano Convention and the provisions of the Brussels Convention, which are substantially reproduced in the Lugano Convention. As this case-note will show, the Norwegian Supreme Court held that the Lugano Convention must be interpreted in the same way as the ECJ ruled in the *Bier* case.[7] Further, the Norwegian Supreme Court found the *Shevill* case[8] "of special interest". It follows that the Norwegian Supreme Court seeks to establish a similar methodological approach as the ECJ. Whether the Norwegian Supreme Court is successful in applying the same methodological reasoning as the ECJ is another question. I will in this case-note comment on the similarities and differences in legal reasoning between the Norwegian Supreme Court and the ECJ. These comments will necessarily be rather vague, as the Norwegian Supreme Court has ruled in very few cases concerning the Lugano Convention. However, this case is more significant than previous cases when it comes to expressed methodological reasoning.

2 Factual background

A broadcasting company, *Sveriges Television AB,* domiciled in Sweden broadcasted from Sweden (on Swedish TV) a documentary produced by a Norwegian journalist domiciled in Sweden. The documentary was made with the intention of showing the restrictions on freedom of speech in Norway. The documentary contained accusations about Norwegian seal hunters violating the Norwegian hunting regulations. The documentary was to a great extent based on a Norwegian person's film, which he and his company were denied the right to show to the public by a Norwegian court. The program was broadcasted twice (2 and 4 February 1994), and could be received by 630 000 people through the Norwegian cable-TV network, and also by a number of recipients in some southern parts of Norway without such connection. Two of the plaintiffs lived in Balsfjord where 186 had cable-TV

---

6 *Antonio Marinari v Lloyd's Bank plc & Zubaidi Trading Company*, C-364/93, ECR 1995, p I-2719, paragraph 16.

7 *GJ Bier BV v Mines de Potasse d'Alsace*, Case 21/76, ECR 1976, p 01735.

8 *Fiona Shevill v Presse Alliance SA*, Case C-68/93, ECR 1995 p I-00415.

connection. One of the plaintiffs lived in Alta where nobody had cable-TV connection. Norwegian seal hunters domiciled in Norway claimed as plaintiffs the accusations to be defamatory. Court litigation was chosen as instrument of redress for the cross border dispute. The plaintiffs sued the defendants in the Norwegian court *Nord-Troms herredsrett*, which rejected to consider the substance of the case based on the procedural reasoning that the court did not have competence to adjudicate the matter according to the Lugano Convention Article 5.3. The decision was appealed on procedural grounds to *Haalogaland Lagmannsrett* which came to the same conclusion. This decision was appealed to *Høyesteretts Kjaeremaalsutvalg*, the Appeal Committee of the Norwegian Supreme Court, which, according to the Law of 25th June 1926, § 6(2), decided that the matter would be a matter for the Norwegian Supreme Court.

3 Legal basis

The Norwegian courts' competence to adjudicate the substance of international civil and commercial matters is regulated by chapter 2 of the Norwegian civil procedural law (the Civil Procedural Act of 13th August 1915 no 6 "om rettergangsmåten for tvistemål") where § 36a decides that the Norwegian civil procedural law chapter 2 is limited by "agreements with a foreign state". Such an agreement is the Lugano Convention, which was ratified by Norway on 2nd February 1993 and adopted and implemented by incorporation as Law of 8th January 1993 no 21 ("Luganoloven"). The law entered into force on 1st May 1993 and regulates international civil and commercial matters between persons domiciled in an EFTA-State and an EU-State. Article 5.3 of the Brussels Convention is equal in wording to the same provisions in the Lugano Convention and the Brussels Jurisdiction Regulation, except for the expression "… or may occur", which was added to clarify the question of whether or not Article 5.3 regulated preventive injunctions pursuant to threatened or incomplete torts, ie, *quia timet actions*.[9]

[9] Work has been undertaken for the revision of the Brussels Convention (and the Lugano Convention), and the Council has approved the content of the revised texts. The preamble of the Brussels Jurisdiction Regulation states that "[c]ontinuity in the results achieved in that revision should be ensured", see paragraph 5 *in fine*.

4 Legal reasoning in light of ECJ case law

The Norwegian Supreme Court was unanimous when deciding that Norwegian courts were competent to adjudicate the matter according to the Lugano Convention art 5.3.

4.1 Establishing the relevance and scope of Article 5.3 as legal basis

Firstly, the Court introduces the Norwegian law incorporating the Lugano Convention into domestic Norwegian law, Law no. 21 of 8th January 1993.

As in the legal reasoning of the ECJ, the court presents the main rule in Article 2 followed by Article 5.3 for matters relating to "tort, delict or quasi delict". However, it does not, as the ECJ, explain the relationship between the main rule in Article 2 and the special jurisdiction in Article 5.3 and the implications for the interpretation of Article 5.3, which is to be considered as an exception to the main rule with a narrow scope and restrictive interpretation.

In contrast to the ECJ, the court presumes, without any assessment, that defamation fulfils the objective requirement pursuant to Article 5.3 *ratione materiae*: the subject matter of the litigation must warrant a different linking factor, and this subject matter is "tort, delict and quasi-delict".

4.2 Establishing the relevant legal question in issue

Secondly, like the ECJ, the court starts with the wording of Article 5.3 and states that according to the Norwegian language version of the Convention Article 5.3, a person domiciled in a Member State can be sued in the courts of the place where the harmful event occurred.

In the Norwegian text, this place is distinctively – and in contrast to the other language versions of the Convention – defined by way of parenthesis, which states that the place where the harmful event occurred is the place where the harmful damage occurred or the place of the event that gives rise to and is the origin of that damage.

The court presents the legal question in issue, asking whether Article 5.3 justifies the attribution of jurisdiction to Norwegian courts and whether the alleged damage occurred in Norway.

4.3 Defining the place of the harmful event and establishing the relevant sources of law

Thirdly, the court states, like the ECJ presumes in its practice, that the Norwegian version of the Convention is equally authentic as the other authentic languages in which the Convention is drafted.

Further, the court establishes the relevance of rulings by the ECJ by referring to the wording of the Danish Lugano Convention stating that it is identical with the wording of the Brussels Convention Article 5.3. The court states that the Lugano Convention must be interpreted in the same way as the ECJ ruled concerning the Brussels Convention in the *Bier* case, where the ECJ stated that the expression "place where the harmful event occurred" in the Brussels Convention Article 5.3 must be understood as being intended to cover both the place of the happening of the event which may give rise to liability and the place where that event results in damage when those places are not identical.

4.4 Establishing the relevance of the Shevill case

Fourthly, the court states that the ECJ decision in the Shevill case "is of special interest". The court explains the facts of the *Shevill* case and cites the Danish version of the ECJ's ruling.

The court states that even though newspapers differ from broadcasting as media, the ruling is relevant and will be of guidance for the court's reasoning. Instead of defining what the differences between newspapers and television are and to what extent the differences may be of legal relevance for the reasoning in this case, based on the special considerations behind Article 5.3 (see below in section 4.5), the court merely states and preliminarily concludes that "applied to the legal issue in question in this case, the *Shevill* case argues in favour for justifying the attribution of jurisdiction to Norwegian courts since the alleged defamatory statements broadcasted in Sweden caused harmful effects in Norway". Further, and in contrast to the ECJ, the court refers, without legal emphasis, to the result in the ruling by the Appeal Committee of the Norwegian Supreme Court concerning the corresponding § 29 in the Law of 13th August no 6 (the Norwegian civil procedure law), where in a

similar case, the Norwegian court was considered as competent to adjudicate the subject matter.[10]

4.5 The legal reasoning pursuant to the special considerations behind Article 5.3

Fifthly, and again in contrast to the ECJ, the court asks after its preliminary conclusion if special considerations can argue in favour for not justifying the attribution of jurisdiction to Norwegian courts. This legal reasoning presumes that Article 5.3 is applicable. It operates with a presumption that the reasoning pursuant to Article 5.3 must be executed in two parts, whereafter, in this case, the court is competent according to the first assessment referred to in section 4.4 above, unless special considerations can argue in favour for not justifying the attribution of jurisdiction to court. This construction operates with a main presumptive rule with an exception thereto and is not in harmony with the approach and legal reasoning of the ECJ, which considers the special considerations behind Article 5.3 as requirements for the applicability of Article 5.3, which all are included in a total, and not separate, assessment.

Because of the confusion of the construction, legal reasoning and content of the special considerations and requirements pursuant to Article 5.3, as they have been developed and defined in case law, I will make a short summary of these requirements. Firstly, the forum called upon to hear the case must find existence of a particularly close connecting factor between the dispute related to "tort, delict and quasi-delict" (which warrants a derogation from the main rule in Article 2) and the court which may be called upon to hear it. Secondly, this forum must show without difficulty the special link justifying such derogation. Thirdly, the designation of forum must establish a rule of jurisdiction according to which Article 2 only is derogated from warranting an application of Article 5.3 in certain clearly defined situations giving Article 5.3 a restrictive scope with a view only to facilitate "the sound administration of justice" (and not the protection of the injured party), which according to the ECJ is the facilitation of the efficacious conduct of the proceedings and the taking of evidence, where thorough investigation into the facts most easily can be carried out, and where the best chances of determining the nature of the relationship in the fullest possible knowledge of

[10] See Rt 1994, p 675.

the facts of the case. Fourthly, this rule of jurisdiction must facilitate "the sound administration of justice" by minimising the possibility of concurrent proceedings and ensuring that irreconcilable judgments will not be given in two Member States hindering the multiplication of the bases of jurisdiction in one and the same case, that would not be likely to encourage legal certainty and the effectiveness of legal protection throughout the territory of the community. Therefore, it is in accordance with the objective of the convention to avoid a wide and multifarious interpretation of the exceptions to the general rule of jurisdiction in Article 2. Fifthly, the designation of forum must establish a rule of jurisdiction that must be highly predictable, easy to identify by the plaintiff and reasonable to foresee by the defendant, encouraging legal certainty and the effectiveness of legal protection throughout the territory. Sixthly, Article 5 is only applicable if the alternative forum decided by the term "in the courts for the place where the harmful event occurred or may occur" is in another state than the state where the defendant is domiciled. If the alternative forum is in the same state as the state where the defendant is domiciled, the matter will then be regulated by Article 2, and the State's national regulation will subsequently determine which of its domestic courts is competent to adjudicate the substance matter.[11]

Further, the court explains that Article 5.3 attributes jurisdiction not only to the courts of a country, but also to the specific courts of the country in question.

The court then assesses whether special considerations can argue in favour for not justifying the attribution of jurisdiction to Norwegian courts. Without specific reference to the requirement for a close connecting factor, the court states that the lack of marketing of the TV program in Norway is of minor significance. Marketing could not in any event be a conclusive connecting factor.

Also, the court rejects the view that protection of the freedom of speech for Swedish Television pursuant to the European Human Rights Convention Article 10 could hinder attribution of jurisdiction to Norwegian courts. Even though this was not a question asked and answered in the *Shevill* case, the court states that this was not a hinder for the ECJ to attribute jurisdiction. Further, the court inserts in its text paragraph 31 of the *Shevill* ruling:

> *In accordance with the requirements of the sound administration of justice, the basis of the rule of special jurisdiction in Article 5(3), the courts of each Contracting State in which the defamatory publication was dis-*

[11] Stephen O'Malley and Alexander Layton, *European Civil Practice* (London: Sweet & Maxwell, 1989), p 369.

> *tributed and in which the victim claims to have suffered injury to his reputation are territorially the best places to assess the libel committed in that State and to determine the extent of the corresponding damage.*

The court argues on the basis of the ECJ's reasoning that this statement could not favour a restrictive interpretation of this part of the convention concerning broadcasting, since this statement would not have any less relevance for broadcasting than for newspapers. However, the court does not assess the substance of differences and similarities between newspapers and television, and to what extent the differences may be of legal relevance for the reasoning in this case, based on the special considerations behind Article 5.3. The court merely states that if the Lugano Convention Article 5.3 was inapplicable to a Swedish broadcasting program, the Article would be inapplicable to broadcasting, and reasons with reference to the ECJ ruling (paragraphs 26 and 27) in the *Shevill* case, that the forum at the place of the event giving rise to the damage will often coincide with the main rule in Article 2, rendering Article 5.3 meaningless unless the attribution of jurisdiction was given to the courts of the place where the harmful effect occurred. The court refers, without emphasis, to legal theory[12] with further references assuming that Article 5.3 is applicable to broadcasting.

The court states further that the fact that Swedish Television had few possibilities to hinder the broadcasting of the program due to its international cooperation agreement on simultaneous and unaltered broadcasting via the cable-TV network, cannot justify not applying Article 5.3 and the attribution of jurisdiction to Norwegian courts. Neither can the court reject the attribution of jurisdiction to Norwegian courts according to Article 5.3 with the reasoning that the Swedish State allegedly would not recognise the judgment according to Article 27.

Finally, the court gave some clarifications on how to distinguish questions of jurisdictional character from questions relevant to the choice of law and the subject matter determined by *lex causae*, since the disputing parties seemed to confuse the distinctions between the questions.

---

[12] Kjetilbjørn Hertz, *Jurisdiction in Contract and Tort under the Brussels Convention* (Copenhagen, 1998).

BOKEN I INTERNETTETS TIDSALDER

JON BING

Det har langsomt gått opp for meg at den moderne boken er resultatet av en rekke oppfinnelser.

Selve boken er en oppfinnelse. Det heter seg at Pergamon ble utsatt fra egyptisk embargo: I den tro at byens bibliotek truet biblioteket i Alexandria i størrelse og ry, forbød man eksport av papyrus som jo bare vokste helt sør i Middelhavet. Da måtte bibliotekarene i Pergamon finne et alternativt kopieringsmedium, og kastet grådige øyne på kalver og geiter som gresset rundt byen. De prepparerte skinnene ble oppkalt etter byen: *Pergament.* Selv om det var kostbart (man måtte jo slakte ett dyr for å få noen sider), så var det likevel mer tilgjengelig enn papyrus.

Og pergament hadde egenskaper forskjellig fra papyrusruller. Det var lettere å forme skjønnskrift, og å dekorere teksten med bilder, farver og bladgull. Og det var tilstrekkelig ugjennomsiktig til at man kunne skrive på begge sider av arket: Det var en kompakt lagring av tekst og bilder. Og bandt man dem sammen, ble resultatet ikke en rull, men en bok!

I de tre-fire første århundrene etter Kristus ble papyrusruller langsomt konvertert til bøker. Pergament ble supplert med klutepapir. Det skjedde en dramatisk konvertering av ruller til bøker, bibliotekarer valgte ut titlene som slik er blitt bevart for ettertiden. Det er antatt at mange tekster gikk tapt i denne prosessen. På en måte er dette en parallell til den konverteringen fra analog til digital form som skjer i våre dager.

I 1985 forberedte man byggingen av et høyhus med leiligheter i den koreanske byen Cheongju. Under gravingen fant man rester av et gammelt tempel, og arkeologer ble tilkalt. De avdekket flere gjenstander, blant annen en stor metalltromme og omtrent tyve leirkrukker for smelting av metall preget med ordet «Heungdeoksa». Dermed hadde man funnet det stedet hvor den eldste kjente boken ble trykket ved hjelp av bevegelige metalltyper.

Denne teknikken ble utviklet under Koryo-kongedømmet (918–1329). Men på grunn av kriger og stridigheter, finnes det ikke lenger noe eksempel på en av de tidlige, trykte bøkene i dagens Korea. Til alles forbauselse ble imidlertid en slik bok vist offentlig for første gang i forbindelse med Det internasjonale bokåret i 1972 ved Nasjonalbiblioteket i Paris. Den hadde vært del av den private samlingen som en fransk diplomat rundt 1900 tok

med seg tilbake til Frankrike, hvor den etter hans død ble solgt til en annen privat samler som igjen hadde testamentert den til Nasjonalbiblioteket, som fikk hånd om boken i 1950.

Denne boken antar man ble til i 1372, nesten hundre år før Gutenberg ga seg i kast med sin bibel. Bokens tittel er lang, men gjengis gjerne i kortformen *Buljo Jikji.* Boken er det andre av to bind med utdrag av buddhistiske hymner, poesi, læresetninger osv samlet av den lærde munken Kyeonghan (1298–1374). Boken ble berømt i samtiden og omtalt som «et klart lys i mørket og en sval bris en het sommerdag».

For å lage metalltypene, ble tegnene skåret ut på raffinert bivoks og pakket inn i gips. Under oppvarming rant voksen ut. Deretter helte man smeltet jern i formene for å støpe typene. Formen kunne ikke brukes på ny, derfor er de samme tegnene ikke identiske.

Selv om Koreas bøker var de første som ble trykt med bevegelige typer, var det Gutenbergs presse som førte til de sosiale omveltningene som boken kom til å representere. Antallet bøker i Europa på den tiden da trykkeripressen ble utviklet er usikkert, ulike kilder angir forskjellige tall – 30 000 bind er ett anslag. Lar man pressene arbeide i ca 50 år, fant man 300 trykkerier – ikke i Europa, men i Venezia, og antallet bøker var økt til ca 15 millioner.

For en jurist er det lett å bli fascinert av hvordan denne første masseproduserte *varen* førte til et sterkt press for å finne en rettslig løsning for regulering av markedet. Visstnok var det også i Venezia denne første gang oppsto, man fant løsningen i de privilegiene som republikken i middelalderen ga handelsmenn. Ved hjelp av et «patent» – dvs en enerett – fikk typisk en trykker enerett til å mangfoldiggjøre en tekst. Teksten kunne være nyskrevet, men var oftere en eldre tekst overført fra en håndskrift, en oversettelse av et klassisk verk osv. Ved hjelp av enerettene ble markedet regulert, trykkeren unngikk konkurranse fra andre som så at en tekst ble populær, og som derfor fikk lyst til selv å trykke den for å få en del av kaken. Enerettene gjorde det mulig å investere i dyre maskiner, i metall og sats for å sette boken og forrente investeringen ved å selge mange bøker til forholdsvis lav pris.

Men bøker var likevel dyre. I det 19. århundre skjedde mye som revolusjonerte markedet for trykksaker. Papir – slik vi i dag kjenner det – ble funnet opp i 1844 av en tysk tekstilarbeider som oppdaget hvordan tremasse kunne bli til billigere papir. Dampmaskiner drev båter og tog over lange avstander, og kunne frakte med seg tunge laster av bøker, tidsskrifter eller aviser: Et større og internasjonalt marked for trykte skrift ble åpnet opp. Rotasjonspressen ble funnet opp, Krimkrigen førte de første fotografiene inn på avisenes forsider, farver ble tatt i bruk. Og det internasjonale markedet for datidens populære forfattere som Victor Hugo, Jules Verne eller Charles

Dickens førte til at man fikk den internasjonale konvensjonen om vern av kunstneriske og litterære verk – Bern-konvensjonen fra 1886.

Men oppfinnelsene sluttet ikke med boken, trykkeripressene, papiret osv. Inn i det 20. århundre forandret boken seg igjen, i Norge fikk man på slutten av 1960-tallet f eks den moderne billigboken med forlaget Pax og Gyldendals lanterne- og fakkelserie som eksponenter.

Grunnen til at en slik komprimert historie av bokens utvikling er relevant i en artikkel om moderne informasjonsteknologi og bøker er tydeliggjøringen at vi i dag ikke har å gjøre med et *brudd* i utviklingen – tvert imot er vi en del av den samme utviklingen som startet da pergament ble skåret i firkanter og brukt til å binde den første boken.

Det første som skjedde med boken ved hjelp av moderne informasjonsteknologi var en revolusjon av *reprografi.* Noen av oss kan huske en tid da det ikke fantes fotokopieringsutstyr, hvor alternativ til forlagsproduksjon var omstendelig spritduplikatorer eller svertestensiler. Fotokopiering gjorde mangfoldiggjøring enkelt, varemerket Xerox ble til verbet «xeroxere». Resultatet ble ikke bøker, men forlagsproduksjonen fikk en konkurranse. Også denne ble rettslig regulert, i Norge ved hjelp av avtalesystemer i regi av forvaltningsorganisasjonen Kopinor som fører en viss vederlagsstrøm tilbake fra de som utnytter reproduksjonsteknologi uten direkte avtale med rettighethaver, til de opphavsmenn som har skapt verkene som gjøres til gjenstand for reproduksjon.

Men det var bare en liten begynnelse.

Noen av oss kan også huske de første tekstbehandlingssystemene. De var klossete og ubehjelpelige. Løsningene var kanskje til nytte for større organisasjoner. Det første tekstbehandlingssystemet for Det juridiske fakultet ved Universitetet i Oslo var et Wang-anlegg anskaffet på slutten av 1970-tallet. Årsaken var en budsjettpost som ikke var oppbrukt ved årets utgang, den passet til anskaffelse av systemet. Den daværende Avdeling for EDB-spørsmål (forløperen til Institutt for rettsinformatikk) hadde allerede utredet spørsmålet ved daværende vitenskapelig assistent Dag Frøystad (som nå er advokat i IBM). Man hadde derfor et ferdig forslag til bruk av de disponible midlene, og systemet ble innkjøpt.

Sentralenheten ble plassert på ett av toalettene, et par sekretærer fikk terminaler og opplæring. Systemet ble ikke egentlig møtt med skepsis, det bare ble oversett, det var noe som ikke angikk de vitenskapelig ansatte.

Jeg mener å huske at vendingen kom med betydelig dramatikk. Professor Carsten Smith satt som leder av banklovutvalget. Etter et flere dagers langt møte la han et lovutkast revidert med håndskrevne endringer i kurven til sin kontormedarbeider, Ellen Kirkerud. Han gjorde det med et sukk, lovutkastet var langt, endringene var mange, av erfaring visste han at det ville ta et par

ukers møysommelig arbeid for Ellen Kirkerud å renskrive utkastet – som så ville bli gjenstand for nye endringer på neste møte.

Da professor Smith kom tilbake fra lunsj, fant han en renskrevet versjon på skrivebordet sitt. Sett fra hans side var dette omtrent like sannsynlig som om Moses skulle ha trådt inn på kontoret med steintavler under armene. Da forklaringen viste seg ikke å være et mirakel, men tekstbehandlingssystemet på toalettet, forstummet enhver antydning om at dette kunne være noe annet enn en velsignelse for jurister i sin alminnelighet og lovgivere i særdeleshet.

Men det var først da IBM lanserte sin Personal Computer basert på en Intel 8088 mikroprosessor i 1981, at revolusjonen kunne skimtes. En typisk PC (varemerket er igjen blitt et substantiv) hadde monokrom skjerm, en sentralenhet på 16K RAM og en (eller to) 5,25 tommers diskettstasjon (faste magnetplatestasjoner ble ikke vanlig før tre år senere).

Men allerede disse første tekstbehandlingssystemene demonstrerte en revolusjon. Den ga en helt ny frihet til forfattere.

Tidligere var rettetasten på skrivemaskinen det største som hadde hendt meg siden jeg begynte å skrive på den utrangerte Royal skrivemaskinen som min far hadde kjøpt fra sin arbeidsplass, Trondheim politikammer. Det var en stor og tung maskin, typene var loddet til typearmen, og «g» satt ikke ordentlig – jeg måtte stadig bruke knipetang for å klemme den fast til armen i et forsøk på å holde den på linje med de andre bokstavene. Den var et treskeverk, og jeg elsket den. På mange måter tror jeg den var grunnen til at jeg begynte å skrive: Jeg hadde stor glede av å bruke maskinen, men for å oppleve denne gleden, måtte jeg jo skrive noe. Resultatet ble *R/S Rollo,* beretningen om romskipet Rollos eventyr i et verdensrom limt sammen av pastisjer fra de få science fiction-bøkene jeg hadde lest til da. Jeg gikk i sjette klasse på folkeskolen, og manuskriptet til *R/S Rollo* står fremdeles i hyllen min, innbundet med brunt limbånd i ryggen.

Selv om jeg elsket skrivemaskinene mine, var de tyranner. Jeg kan huske problemene med å få farvebåndet til å løpe riktig, timer brukt til å fjerne limbåndet som rettetasten brukte for å løfte avtrykket av en bokstav bort fra papiret, men som alt for ofte tvinnet seg inn i andre av maskinens deler. Bare de som har slike minner skjønner riktig å sette pris på et tekstbehandlingssystem, hvor man ikke behøver å skifte ark ved bunnen av en side, hvor det alltid er plass til en fotnote til, et system som har gjort «blåpapir» til et ord like gammeldags som «pergament». Et system som gjør at man kan sette inn et nytt ord eller avsnitt uten å skrive om manuskriptet (og mange av oss ville gjerne ha pene manuskripter, så vi skrev dem om). Hvis noen føler at prosaen nå bæres opp av en lyrisk undertone, så er det helt korrekt – tekstbehandlingssystemene frigjorde forfattere fra den rette linjens tyranni, fra A4-arkets trange fengsel. Kanskje gjorde de oss også

mindre økonomiske når det gjaldt ord (for det er så lett å skrive ett til), men spill gjerne skribentenes frigjøringsmarsj på de første personlige datamaskiners tastatur.

Jeg demonstrerte selv denne frigjøringen i forbindelse med utgivelsen av ungdomsromanen *Mizt – gjenferdenes planet* (Damm 1984). Den ble skrevet på en liten datamaskin, ikke en «PC», men en Facit/Addo 800 DTC. Den hadde en dobbelt diskettstasjon for 5,25 tommers disketter, på den ene var tekstbehandlingssystemet, på den andre ble teksten lagret. Ved hjelp av urimelig innsats fra en leverandør som nå også tilhører fortiden (Alf G Johnsen) ble teksten overført over et TTY-grensesnitt på oppringt linje ved hjelp et 300 bauds modem til Lovdata. Her ble teksten etterbehandlet på deres Nord-10/S anlegg ved hjelp av programmer Lovdata brukte for å produsere lovtekst – det ble lagt inn sidebeskrivningskoder som hadde samme funksjon som nå er bedre kjent fra SGML eller HTML. Her ble også rettskrivningen kontrollert ved egenutviklede staveprogrammer (TRANS). Det ble tatt ut korrektureksemplar på papir, forlag og forfatter leste korrektur på vanlig måte. Så ble teksten overført til et magnetbånd, og teksten ble fotosatt og ombrukket av Dataprint as (også et selskap i fortiden).

Så vidt jeg vet var dette første gang en norsk forfatter selv på denne måten produserte trykkegrunnlaget for egen bok. Det lyder kanskje klossete og tungvint, men var en befrielse – det ga egenkontroll, og som forfatter så man hvordan datamaskinen eliminerte store deler av den infrastruktur som til vanlig ikke bare var til støtte, men også til hinder for å gjøre ting nøyaktig slik man selv ville ha dem. Tyve år etter dette eksperimentet er mesteparten av de tradisjonelle organisatoriske rammene der fremdeles, men likevel … de er bygd på sviktende forutsetninger.

Én åpenbar endring er grafikk. Etter at de illuminerte, håndskrevne bøkene ble presset til side av billigere trykksaker, har bøker vært fattige på illustrasjoner. Illustrasjoner var både vanskelige å fremstille og fordyret produksjonsprosessen. Dessuten hadde ikke forfatteren (eller andre) hjelpemidler til å lage illustrasjoner på samme måte som skrivemaskinen var blitt et hjelpemiddel for å skrive. Selv et enkelt flytdiagram var det vanskelig å fremstille, og ville typisk forutsette produksjon av en klisjé, i alle fall en rentegning for offset (jeg tilbyr gjerne min egen bok *Rettslige kommunikasjonsprosesser,* Universitetsforlaget 1982, som eksempel). Også her har datamaskinen ført til en revolusjon. Nå er ikke de forfattere som dominerer markedet i dag oppvokst med mulighetene under fingrene, derfor er de heller ikke tatt i bruk slik man kan vente at de vil bli i en fremtid hvor man bevisst velger tekst eller grafikk (eller noe annet) ut fra forholdet mellom mål og middel. De gjennomillustrerte fagbøkene – hvor illustrasjonene ikke

er billedlig atspredelse, men diagrammer, dokumentasjon, referanser osv – har ennå ikke tonet frem i all sin overbevisende velde, men de er på vei.

Datamaskinsystemene er noe mer enn maskiner som gjør det lettere å produsere bøker. De er et alternativ til bøkene. I 1984 skrev jeg en liten essaysamling som ble kalt *Boken er død! Leve boken!* (Universitetsforlaget), en tittel som spilte på dobbeltbetydningen av ordet «bok». De kunne jo være fristende å spørre om den påstanden tittelen impliserer, er realisert. Og det er lett å konstatere at den tradisjonelle boken lever i beste velgående, den er ikke blitt erstattet av *e*-bøker.

Det er sant, men også for unyansert. Jurister har for eksempel hatt alle primære rettskildefaktorer som lover, forskrifter, høyesterettsdommer mv tilgjengelig i Lovdatas direktekoblet system fra 1981. Symbolet for jus i Norge er den røde lovboken, Norges lover. Jeg husker ikke sist jeg slo opp i den, det er sikkert måneder siden. For Lovdatas base med gjeldende lover ligger bare ett tastetrykk unna. Det er raskere å få opp søkebildet enn å løfte boken ned fra hyllen. Og i boken tar det tid å lete seg frem, selv det å bla opp en lov man vet hvor finnes, tar tid. Og har man funnet den, og skal sitere teksten i en artikkel man arbeider med, har boken forferdelig dårlige klipp-og-lim funksjoner. Dessuten er den foreldet, minst med ca ett halvt år. Boken er rett og slett for tungvint, derfor bruker jeg den ikke.

Og det er selvsagt den prøve også *e*-boken må møte. Den vil ikke erstatte papirboken før den blir lettere, mer tiltrekkende å bruke. Den er nesten det i dag – en leseplate med skrift bestemt av leseren (størrelse, typesnitt), søkbar, med mulighet for å gjøre notater hvor som helst, men innebygd ordbok og leksikon, og hvor leseplaten er opplyst bakfra så man alltid har godt leselys. Det kan lagres minst et snes bøker i platen, og minnebrikker store som kronestykker kan inneholde flere titler. *E*-boken er faktisk et brukbart alternativ allerede.

Og naturligvis inneholder *e*-boken mer enn tekst og bilder, den inneholder musikk (den er f eks en MP3-spiller), tale og levende bilder. Den er egentlig ikke en «bok» i den betydning at den er en avgrenset enhet med data. Den er et grensesnitt mot Internettet (eller hva vi etter hvert vil kalle det verdensomspennende nettverket). Derfor gir kanskje ordet «bok» en uriktig metafor, for det speiler bare ett aspekt ved den enheten vi bruker til å lese tekster på, spille spill mot, få nyhetene servert på, lytte til musikk, ringe opp venner for å sende dem et foto av der hvor du er akkurat nå. Denne enheten strever i dag med å finne sin form – de mest populære eksemplene kalles mobiltelefoner eller personlige elektroniske assistenter (PDA). I dag har vi alle minst en av hver (sommeren 2003 hadde hver nordmann i gjennomsnitt ett mobiltelefonabonnement). Hvem vet om de smelter til én eller splittes til

mange funksjonelt spesialiserte enheter. Hvem vet om de forblir utenfor kroppen, eller integreres.

Kanskje fremtidens *e*-bok vil være et lite ikon du kan se når du med lukkede øyne skjeler nedover til høye. Og kniper du øynene sammen, åpner ikonet seg og teksten i Odysseen eller en annen valgt tittel vises for ditt bokstavelige talt indre blikk.

FORFATTEROPPLYSNINGER

Jon Bing (<jon.bing@jus.uio.no>) er professor og tidligere bestyrer ved Institutt for rettsinformatikk. Han er dr. juris (Universitetet i Oslo 1982), dr. juris hon. causae (Stockholms universitet 1997), dr. juris hon. causae (Københavns universitet 1998), Visiting Professor ved King's College i London og leder for Personvernnemda i Norge. Han arbeider særlig med personvernrett, immaterialrett og interlegal rett.

Lee A. Bygrave (<lee.bygrave@jus.uio.no>; <http://folk.uio.no/lee/>) er dr. juris (Universitetet i Oslo 2000). I tillegg har han B.A.(Hon.s) og LL.B.(Hon.s) fra Australian National University i Canberra. Han er førsteamanuensis ved Institutt for rettsinformatikk, hvor han i hovedsak arbeider med forbrukervern- og personvernspørsmål knyttet til e-handel.

Georg Philip Krog (<g.p.krog@jus.uio.no>; <http://folk.uio.no/georgpk>) er cand. jur (Universitetet i Oslo 2000). Han er doktorgradsstipendiat ved Institutt for rettsinformatikk hvor han arbeider med spørsmål vedrørende internasjonal privatrett. Han er for tiden gjesteforsker ved Stanford Law School.

Rolf Riisnæs (<rolf.riisnas@jus.uio.no>; <http://folk.uio.no/rolfriis>) er cand. jur (Universitetet i Oslo 1994). Han er doktorgradsstipendiat ved Institutt for rettsinformatikk hvor han arbeider med rettslige spørsmål knyttet til elektronisk signatur og sertifikattjenester (TTP/PKI), elektronisk handel, elektronisk datautveksling (EDI), elektronisk saksbehandling /forvaltning og personvern.

Emily M. Weitzenböck (<emily.weitzenboeck@jus.uio.no>; <http://folk.uio.no/emilyw/>) er doktorgradsstipendiat ved Institutt for rettsinformatikk. Hun har LL.M. fra Universitetet i Southampton, England og LL.D. fra Universitetet i Malta. Hun arbeider primært med selskaps- og kontraktsrettslige spørsmål knyttet til virtuelle organisasjoner og liknende samarbeidsformer.

NOTES ON AUTHORS

Jon Bing (<jon.bing@jus.uio.no>) is professor and former head of the NRCCL. He has the degrees of dr. juris (University of Oslo, 1982), dr. juris hon. causae (Stockholm University, 1997), dr. juris hon. causae (Copenhagen University, 1998). Amongst numerous engagements, he is chair of the Data Protection Tribunal in Norway and Visiting Professor at King's College, London. His main fields of research are privacy/data protection law, intellectual property rights and private international law.

Lee A. Bygrave (<lee.bygrave@jus.uio.no>; <http://folk.uio.no/lee/>) was awarded the degree of dr. juris at the University of Oslo in 2000. In addition, he has a B.A.(Hon.s) and LL.B.(Hon.s) from the Australian National University, Canberra. He is presently Associate Professor at the NRCCL, where he works primarily on consumer and privacy/data protection issues connected with e-commerce.

Georg Philip Krog (<g.p.krog@jus.uio.no>; <http://folk.uio.no/georgpk>) has the degree of cand. jur from the University of Oslo (2000). He is a doctoral research fellow at the NRCCL where he works primarily on issues related to private international law. At present, he is a visiting scholar at Stanford Law School.

Rolf Riisnæs (<rolf.riisnas@jus.uio.no>; <http://folk.uio.no/rolfriis>) has the degree of cand. jur from the University of Oslo (1994). He is a doctoral research fellow at the NRCCL where he works on legal issues related to electronic signature and certificate services (TTP/PKI), electronic commerce, electronic document interchange, electronic administration and privacy/data protection.

Emily M. Weitzenböck (<emily.weitzenboeck@jus.uio.no>; <http://folk.uio.no/emilyw/>) is a doctoral research fellow at the NRCCL with an LL.M. from the University of Southampton, England and an LL.D. from the University of Malta. She works primarily on corporate and contractual legal issues related to dynamic, networked organisations such as virtual organisations.