

e-Commerce 2003: Netherlands

Dinant T.L. Oosterbaan, Christiaan A. Jeekel and Louis Jonker

in: *Getting the Deal Through: e-Commerce 2003 in 25 jurisdictions worldwide*
London: Law Business Research Ltd. 2003, p. 123

1. *How can the government's attitude and approach to Internet-related issues best be described?*

Over the last few years, the Netherlands government has published several policy documents and action plans to promote electronic commerce. The purpose of its 1999 policy paper 'The Digital Delta - The Netherlands Online', is to promulgate several action plans intended to give concrete form to the ambition of the Netherlands to be part of an European Internet leadership group. According to 'The Digital Delta', the Netherlands wants to remain part of the worldwide information elite. In 2000 the Netherlands government introduced its e-commerce project 'Netherlands goes digital', which is still continuing.

Having adequate legal certainty for the Internet, and in particular removing any legislative or regulatory obstacles, is an important part of government policy. In February 1998 the Netherlands government issued a wide-ranging 207-page discussion paper on new legislation for the electronic highway. In 2000, the Ministry of Justice published more specific guidelines on internationalization and law in the information society. Finally, there are several projects with respect to electronic government and to constitutional rights in the digital era.

2. *Which, if any, regulatory bodies are responsible for the regulation of e-commerce and Internet access tariffs and charges?*

In the Netherlands no regulatory bodies are responsible for the regulation of e-commerce. It is worth mentioning that, as a continuation of existing electronic data interchange-initiatives, the so-called Electronic Commerce Platform Netherlands was launched to promote e-commerce activities, including a self-regulatory e-commerce code of conduct.

Although it may be argued that the Internet is technically not covered by the present Telecommunications Act, the Netherlands telecommunications regulatory agency OPTA issued several position papers and decisions on Internet-related matters including Internet access and interconnection, Internet access tariffs and charges and co-location. Obviously, the EU Directives of March 2002 on electronic communication networks and services and the adaptation of the Netherlands Telecommunications Act proposed in November 2002 will play a determining role in the future.

3. *What legislation/other acts govern business on the Internet?*

The government generally takes the view that legal rules relevant in the physical world should also be relevant in the electronic domain: what applies offline should also apply online. It thus comes as no surprise that general legislation such as the Civil Code, the Code of Civil Procedure, the Copyright Act, and the Competition Act also govern business on the Internet. E-commerce-related EU Directives have been implemented in Dutch legislation in accordance with the chart presented at the end of this paper.

4. *What tests or rules are applied by the courts to determine the proper jurisdiction for Internet-based transactions (or contentions) in cases where the defendant is resident or provides goods or services from outside the jurisdiction?*

Much has been written about the three major international legal issues of Internet-related transactions: applicable law, jurisdiction and the enforcement of judgments. However, with respect to e-commerce business transactions, e-commerce consumer transactions, Internet criminal law and Internet unfair competition law, case law is lacking. There is substantial case law in matters of Internet-related intellectual property but generally under Dutch law.

Private international law for contractual relationships is governed by the rules of the 1980 Rome Convention on the law applicable to contractual obligations. The rules of the Convention sanction explicit choice-of-law clauses. If the law of no particular country is chosen, the law of the country with which the contract is most closely connected will govern the contract. This is usually the principal place of business of the party which is to effect the contract. According to Article 5 of the Rome Convention, passive consumers in Internet transactions may be protected by the mandatory rules of Dutch law, but it is debatable whether Internet consumers can be considered passive consumers under Article 5.2 of the Rome Convention. It is noted that the EU E-commerce Directive does not establish additional rules on private international law.

Since 1 March 2002 international jurisdiction and execution of judgments is governed by the EU Regulation of December 2000. For consumers, including Internet consumers, the EU regulation uses a 'country of destination'-principle which is contrary to the 'country of origin'-principle of the EU E-commerce Directive. It is not to be doubted that conflicts will arise. As far as unfair competition is concerned, including Internet related advertising, the EU regulation uses the 'marketplace'-principle as an alternative forum. Jurisdiction in the relations between the Netherlands and non-Member States is governed by the internal Dutch rules on jurisdiction. Enforcement of a judgment of a Netherlands court may present difficulties outside Convention Member States, as there are few treaties with other countries. No specific Internet-related rules apply.

From a general perspective the following should also be noted. In the Netherlands, the Code of Civil Procedure governs the civil procedure. Unlike US or UK litigation, pre-trial discovery is an unknown concept. In high-tech litigation, courts often appoint independent experts to advise the court on technical issues. Although actual court papers have to be in

Dutch, supporting documentation can be in foreign languages generally understood in the Netherlands such as English, German and French. Many disputes between parties in the information technology and Internet industries are adjudicated in so-called summary proceedings (*kort geding*). Summary proceedings are primarily used to obtain injunctive relief in unfair competition, intellectual property, and contractual disputes. The proceedings consist of an oral hearing before the presiding judge of a district court. The hearing lasts for a few hours and is based on written summons, submission of documents, and oral and written pleadings by the attorneys for parties. These proceedings make it possible to obtain judgment within a short time (one week to two months). The judgment can be executed even if an appeal is filed. The disadvantage is that there are limited possibilities to hear witnesses and experts, although affidavits of witnesses and so-called party experts can be introduced as documentary evidence.

5. *Is it possible to form and conclude contract electronically? If so, how are contracts formed on the Internet?*

According to the Civil Code contracts are generally formed when an offer has been accepted. This can happen orally, in writing, by mail, fax and also electronically as another more modern means of telecommunication. As the Netherlands generally has an open system of proof, the existence of a contract can be proven by any reasonable means. Most contracts do not have formal (written) requirements. However, a few specific contracts, such as insurance agreements, do require a written document. The rationale is primarily to protect the weaker party against himself and against the other party. In our view, individual circumstances determine whether contracts that formally have to be concluded in writing, may under certain circumstances also be concluded electronically. Such individual circumstances are, for instance, whether the rationale has been taken into account and the frequency with which contracting parties communicate electronically. To protect consumers, an electronic distant contract is required to be followed by a paper version.

6. *Are there any particular laws that govern contracting on the Internet? Do these distinguish between business-to-consumer and business-to-business contracts?*

As there is no specific legislation on contracting on the Internet, normal law, in particular the Civil Code, is applicable. The Civil Code does not generally distinguish between business-to-consumer and business-to-business contracts. However, Articles 6:231-247 of the Civil Code contain specific regulations on the applicability of General Terms and Conditions with respect to consumer contracts. Book 7 of the Civil Code on purchase contracts also contains specific provisions on consumer purchase contracts. These provisions are for the protection of consumers. According to the Act of 21 December 2000 to adapt Netherlands legislation to the EU Distant Contracts Directive clear quotations have to be made and consumers should be given time to think the matter over. However, an extensive report by Consumers International, an umbrella organization of consumers' associations, reveals that the situation in the Netherlands is not quite in accordance with the applicable law on distant contracting. For example, only 15 per cent of Dutch webstores inform the consumers about their right to withdraw.

There are several self-regulatory codes with respect to contracting on the Internet. These include the Code of Conduct of the Electronic Commerce Platform Netherlands, regulating conditions, techniques and standards for all users of the Internet. These rules apply to all users of the Internet (consumers, companies, providers, etc) and can therefore be regarded as rules concerning business-to-business contracts, as well as rules concerning business-to-consumers contracts. The Webtrader Code of the Consumers' Association regulates purchasing by consumers on the Internet. These rules apply to purchase contracts by consumers and can therefore be regarded as rules concerning business-to-consumer contracts. As of January 2002 the Webtrader project is no longer active. Finally, the Thuiswinkel.org Code of the Dutch Organization for Home Shopping also regulates purchasing by consumers on the Internet. It can be regarded as establishing rules concerning business-to-consumers contracts. Due to the fact that the Webtrader project is no longer active, the Thuiswinkel.org Code has taken the place of the Webtrader Code.

7. *How does the law recognize or define digital or e-signatures?*

It is generally accepted that signatures must be made in the handwriting of the individual. Many functions of a signature have been identified of which the main function is concerned with proving identity. It is uncertain whether existing electronic signature techniques can fulfil these functions. It is proposed that a combination of several measures, either based on information technology or on other techniques, will ensure that an electronic signature may fulfil all the functions of a handwritten signature. At present there is no specific legislation or case law giving electronic signatures equal status to written signatures. On the basis of the EU Directive on Electronic Signatures a legislative proposal for Electronic Signatures Act was submitted in May 2001, which has been amended in January 2002. This future Act will amend the Civil Code, the Telecommunications Act and the Economic Offenses Act, resulting in the situation that, among others, an electronic signature has the same legal status as a written signature, but only when the method used to verify its authenticity is sufficiently reliable.

8. *Are there any data retention/software legacy requirements in relation to the formation of electronic contracts?*

On the basis of several laws (Article 2:10 Civil Code, tax laws), legal persons and companies have an obligation to retain records, either in physical or in electronic form. The term for such retention is seven years. If records are retained in electronic form, the electronic media must meet necessary technical requirements enabling it to carry the data for the compulsory term and to convert the data when needed. The obligation to retain records, however, does not affect the electronic formation of contracts on the Internet.

9. *What measures must be taken by companies/ISPs to guarantee the security of Internet transactions?*

One must distinguish between general security and privacy. On the basis of the Telecommunications Act, providers of telecommunication networks and providers of

telecommunication services must take all reasonable technical and organizational measures in order to secure their networks and services and also in order to secure the interests of their subscribers and users as regards their personal data and private lives. These measures must guarantee an appropriate level of security in proportion to the applicable risk, taking into account the state of technology and the costs of undertaking these measures.

Under the Personal Data Protection Act, someone responsible for processing personal data (such as ISPs) must take all reasonable technical and organizational measures in order to secure such personal data against unlawful use. There are no specific rules on the measures to be taken by ISPs to ensure security and privacy of Internet transactions. Several possible technical security measures have been identified, including whether these security measures comply with the legal requirements regarding safety and privacy as contained in the Telecommunications Act and the Personal Data Protection Act. In addition, the Dutch Association of Internet Providers has issued self regulatory 'recommended practices' regarding safety for its members. In our view, an ISP will have to take a variety of security measures.

At the same time ISPs have an obligation to make their networks accessible to law enforcement agencies. A legislative proposal with respect to the accessibility to law enforcement agencies of traffic and user data was introduced in October 2001, which proposal was amended in July 2002. In February 2002 the Act on Information and Security Agencies 2002 entered into force, regulating among other things the authorization for the national security service to tap telecommunication traffic data for the sake of national security.

10. *As regards encrypted communications: can any authority require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?*

In the 1998 policy paper of the Netherlands government regarding new legislation for the electronic highway, it is mentioned that the use of encryption is in general allowed. However, for prosecution purposes, the Dutch government has developed a two-tier policy on the availability of private keys. First, within the framework of a government project called 'TTP.NL' started in 1998, in which recommendations are given on the reliability of electronic data interchange and the role of TTPs as certification authorities, it is investigated whether prosecution authorities should have a legal basis to have access to private encryption keys. In a later report on legal access, it is concluded that such access is at present not economically feasible due to the major costs involved for the TTPs. Second, existing prosecution laws (the Criminal Procedures Act and the Act on Information and Security Agencies of 2002) provide sufficient legal basis for access to private keys. Within the framework of general criminal law (Article 125k, Code of Criminal Procedure), third parties who are not suspects can be required to cooperate in de-encrypting data and are thus required to make private keys available. On the basis of articles 17 and 24 of the Act on Information and Security Agencies of 2002, suspects are obliged to cooperate on the making available of private keys in the event national security is at stake.

There is at present no specific legislation with respect to trusted third parties (TTP) and certification authorities. In January 2000 interim results of the aforementioned government project 'TTP.NL' were presented. The government had the intention to establish a so-called TTP Chamber, an umbrella organization bringing together government representatives as well as suppliers and users of TTP services on a voluntary basis. TTPs will provide services to enhance the reliability of electronic data interchange; TTPs and others may fulfil the role of a certification authority. In January 2001 however, this intention of the government was abandoned. European developments, such as the European Signature Standardization Initiative and the development of a Qualified Certificate Policy (QCP), are the reason for the delay of the TTP.NL-project. It is expected that further developments will take place in 2003.

The new Act implementing the EU Directive on Electronic Signatures will regulate the liability of trusted third parties, or 'certification service providers' as they will be called in the new Act. It is proposed to include specific provisions on the liability of certification service providers in the Dutch Civil Code on the basis of which certification service providers are assumed to be liable for possible damages occurred by individuals who have relied on a certificate issued by a certification service provider. Certification service providers will also be liable in the event they failed to register a withdrawal of a certificate. However, certification service providers are allowed to prove that they did not act negligently in such events. When issuing a certificate, certification service providers are permitted to include limitations on the use and the total value of transactions based on the certificate. Exceeding these limitations by individuals does not lead to liability of the certification service provider.

11. *What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?*

The Stichting Internet Domeinregistratie Nederland (the Foundation for Internet Domain Registration in the Netherlands) is responsible for the allocation of Internet domains. The Foundation assigns the .nl country code top-level domain names on a first come, first served basis. According to the most recent and not very restrictive regulations of the Foundation (effective as of 29 January 2003), it is possible for companies and for individuals to register .nl top-level domain names. Residency in the Netherlands is not required although a postal address in the Netherlands has to be appointed, for example the address of a law firm providing domiciliation services, to which (court) documents can be served or sent. Also an administrative contact person (including e-mail address) has to be appointed; based on the regulations of the Foundation, e-mail sent to this administrative contact person is considered to be received by the domain name owner.

The applicant for a domain name must conclude a registration contract with the Foundation in which the applicant, among other things, declares that the domain name does not infringe any rights of third parties, such as trademark or trade name rights. In the signed registration

contract an applicant also declares that it will indemnify the Foundation against possible claims by third parties.

With its most recent regulations the Foundation has also introduced arbitration as a form of alternative dispute resolution. The Arbitration and Mediation Center of the WIPO in Geneva will perform the arbitration. Any party whose trademark or trade name rights are infringed by a .nl domain name owner is entitled to start an arbitration procedure, but is also entitled to start 'normal' litigation with applicable Dutch courts. In the event arbitration is chosen, domain name owners whose .nl domain name has been registered, moved or altered after 29 January 2003 are obliged to accept the decision of the WIPO.

12. *Do domain names confer any additional rights (for instance in relation to trademarks or passing-off) beyond the rights that naturally vest in the domain name?*

The legal status of domain names remains uncertain. Domain names are not yet viewed as separate and distinct (intellectual) property rights. However, it is to be expected that a prior existing domain name may be used to oppose a later abusive registration of a trademark or the later use of a confusingly similar trade name by a third party.

13. *Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?*

The registration and use of Internet domain names has already given rise to almost 200 court judgments. The ownership of a trademark and/or a trade name (under Dutch law trade names are also recognized as intellectual property rights) have proven to be strong arguments in successfully challenging registrations of similar domain names, including pirate registrations. The trademark or trade name owner in such proceedings asks the court to decide that the applicant has to shut down the relevant website immediately; in addition the domain name has to be transferred to the trademark or trade name owner or has to be removed from the domain name register. Additional circumstances are taken into account by the court, such as the true intention of the domain name owner at the time of applying, the distinctiveness of the trademark or trade name, the actual use of the domain name by publishing a website, if applicable the content of the 'pirate' website, and the interests of both parties in the domain name. In most cases, trademark and trade name owners have succeeded in challenging similar domain name registrations by third parties.

There have been several exceptions to the general rule that domain names have to be transferred. The court dismissed a claim by the owner of the trademark 'Ariel', because the registrant only used the domain name for personal purposes and had no intention of selling the domain name for a substantial amount of money. A more or less identical case is *Labaratoire Garnier v Roos Automatisering*. Roos Automatisering had not yet used the domain name 'garnier.nl', but was planning to use it for a music website dedicated to the artist Laurent Garnier. The Court decided that the use of the word 'Garnier' did not infringe the trademark rights of Labaratoire Garnier, because Roos Automatisering did not act without a valid reason. In the *Bravilor v Bouman* case the Court decided that a dealer

does not need permission to use the trademark of the principal as a '.nl' domain name for advertising purposes. It may be argued that this decision is not entirely correct.

14. *What rules govern advertising on the Internet?*

Self-regulation is the generally preferred method of regulating the fast-changing Internet environment. In the Netherlands, there have been several experiments with Internet self-regulation including the regulation of Internet advertising. In October 2001 the Electronic Commerce Platform of the Netherlands (ECP.NL) introduced the latest version of its Model Code of Conduct for Electronic Business. The Dutch Organization for Home Shopping also promulgated a code of conduct known as the Thuiswinkel.org code. These codes are meant for those companies who make offers for their products and services on the Internet to Dutch consumers. In these codes it is mentioned that advertising and promotional messages by third parties on Internet pages must be clearly recognizable as such.

Advertising and promotional activities should not be in violation of Netherlands legislation and the Netherlands Advertising Code. The policy of the EU can be characterized as being in favor of self-regulation. The EU E-commerce Directive provides only minimal regulation.

Regulations on unsolicited advertising, or 'spam', are partially overlapping and partially contradictory. It is unclear whether an opt-out or an opt-in regime for 'spamming' applies, especially in case of 'spamming' by means of e-mail. According to the government an opt-out regime applies, meaning that 'spamming' is allowed unless a notice of objection to receiving 'spam' is received. However, the Telecommunications Act and the Act to adapt Book 7 of the Civil Code concerning the protection of consumers in respect of distance contracts prescribe an opt-in regime when 'spamming' occurs by means of an automatic calling system, meaning that in those cases 'spamming' is only allowed with the prior permission of the receiving party. In future an opt-in regime is expected as the recent EU Directive of July 2002 (the 'Spam and Cookie Directive') is in favor of an opt-in regime. In a case in interim proceedings of the *Dutch government v Matthias Rath* the District Court already applied the opt-in regime of the 'Spam and Cookie Directive' by deciding that Matthias Rath acted unlawfully by sending large quantities of unsolicited e-mail of a commercial nature to members of the Dutch parliament. In another case of *Ab.Fab v XS4ALL* the Court of Appeals still applied the opt-out regime.

When copyright protected music is used in Internet commercials, the permission of the copyright owner is needed. The Netherlands collecting society Buma/Stemra has issued standard contracts, which are to be concluded between Buma/Stemra and the publisher or producer of the commercial when copyright protected music is being used, for example in webcommercials or e-cards. Buma/Stemra was the first collecting society in Europe to introduce standard contracts with regards to Internet.

15. *Are there any products/services that may not be advertised or types of content that are not permitted on the Internet?*

Advertising of certain products is limited or prohibited. For example, the Tobacco Act prohibits almost any form of advertising. Advertising for products like alcohol, drugs and medicine is also restricted. These general rules with respect to advertising also apply to advertising on the Internet. Obviously child pornography and other content infringing criminal law are also prohibited.

16. *Is the advertising or selling of financial services products to consumers or to businesses via the Internet regulated, and if so by whom and in what manner?*

There is much general legislation regulating the advertisement and sale of financial services and products, including the Act on Consumer Credit, the Act on the Supervision of Credit Institutions and the Act on the Supervision of Insurance Companies. There are also self-regulatory rules, such as the Code of Conduct on Financing by Mortgage and the Code of Honor of the Association of Financing Companies. This legislation and the codes of conduct contain protections for consumers such as withdrawal, time to think the matter over, dispute settlement and so forth. In 1999, the Netherlands Central Bank issued specific Policy Guidelines on offering financial services through the Internet and other modern media. The same is true for guidelines promulgated by the Authority Financial Markets (AFM).

Specific legislation on advertising or selling of financial services via Internet is as yet not available. Article 46i of Book 7 of the Dutch Civil Code states that the provisions on consumer protection with distance contracts do not apply to the offering of financial services. The reason for this is the EU Directive on the distance marketing of consumer financial services of 23 September 2002. A legislative proposal to implement this Directive is as yet not available.

17. *Are ISPs liable for content displayed on their sites?*

The liability of ISPs for content displayed on their sites may range from civil liability, under contract and tort law, and intellectual property infringements through to criminal liability. The government generally follows the principle that the same principles apply online and offline.

In line with common Dutch practice, several questions have been raised in litigation. In 1991, the first proceedings concerning criminal liability for software copyright infringement committed on the Internet through a BBS took place. Clearly, unlawful content with respect to child pornography and racism are subject to criminal law. A Center for Child Pornography on the Internet has been set up by several ISPs as a method for self-regulation, which includes shutting down sites and making complaints to the prosecuting authorities. As a member of the Internet Hotline Providers Europe Association (Inhope), the Dutch center cooperates internationally with other centers. A Center for Discrimination

on the Internet has also been set up. Future amending legislation to the EU E-commerce Directive will contain new regulation on the criminal liability of ISPs. Under this new legislation ISPs will not be prosecuted when they execute an order of the public prosecutor, issued with the written authorization of an examining judge, to take all reasonable measures to make the unlawful content inaccessible to the public.

Whether ISPs can be held liable under civil law for content on their sites has been addressed in the significant *Scientology* case. In its 1999 decision on the merits, after initial preliminary injunction proceedings resulting in a 1996 judgment, the The Hague District Court decided the following: “The Court declares it to be the law that by having a reproduction of the works that Scientology has the copyright to on their computer systems, without the consent of the plaintiffs, the ISPs are acting unlawfully if and insofar as they have been notified of this, and moreover the correctness of the notification of this fact cannot be reasonably doubted, and the ISPs have then not proceeded to remove this information from their computer system at the earliest opportunity, or at least to make this information inaccessible”.

Future amending legislation to the EU E-commerce Directive will be relevant in deciding cases regarding the civil liability of ISPs, containing an obligation for ISPs to remove or make inaccessible unlawful content promptly after they have become aware of the unlawful nature of the content. This future legislation has already given rise to discussion in the case of *Deutsche Bahn v XS4ALL*, in which the Court of Appeals in interim proceedings decided that XS4ALL acted unlawfully by not removing the unlawful content promptly; the content was clearly of an unlawful nature. However, the Court also referred to a government explanatory memorandum stating that in general ISPs do not have an obligation to remove or make inaccessible unlawful content promptly after receiving a notice from a third party.

18. *Can an ISP shut down a web page containing defamatory material in the absence of court authorization?*

Depending on the contract with the subscriber, an ISP can shut down a web page containing defamatory material in the absence of a court authorization. As has already been decided in the *Scientology* case and as will be regulated in future amending legislation to the EU E-commerce Directive, ISPs may have the obligation to remove or make inaccessible defamatory material promptly after becoming aware of the defamation.

19. *Can a website provider use third-party content on its website without permission from the third-party content provider?*

A website provider cannot use third-party content on its website without the permission of that content provider where the content is protected by intellectual property rights. In the case of three freelance journalists, the District Court of Amsterdam decided that republishing articles on CD-ROM and the Internet should be considered an independent new reproduction requiring prior permission by the authors. Another interesting case with

an international dimension is *KPN v Kapitol Trading*. The defendant, Kapitol, opened a website on a server located in Belgium containing copies of the Dutch telephone directory. By putting this website on the Internet, the telephone directory was thus made available to the Dutch public. The President of the District Court decided that the use of the KPN directory infringed the copyright of 'non-original' writings of KPN. KPN could therefore resist the copying and publishing of its directories on the website of Kapitol.

In 1999, the Netherlands implemented the EU Database Directive. A very interesting case in which the Database Act has been used is *NVM v De Telegraaf*. The Dutch newspaper De Telegraaf owns a website called El Cheapo where visitors can search for the best bargains on various products. After completing several search criteria and clicking on the search button, El Cheapo searches the Internet on the basis of these search criteria. In this case, among others, the database of the Dutch Real Estate Agents Association (NVM) was searched. The search result will be copied to the server of El Cheapo and then presented on the screen of the visitor. According to the Court of Appeals, the data files of NVM are not a database under the Database Act, because they are just a spin-off of the main activities of NVM. Therefore De Telegraaf did not infringe any database rights of NVM. However, the Supreme Court dismissed the spin-off argument and stated that NVM's database is a database as protected under the Databases Act; a database may be used for multiple purposes so that an additional substantial effort to produce an online database which is based on an offline database is not required.

Another interesting, but more specific case is the *Kranten.com (Newspaper.com)* case. Several newspapers accused Internet company Eureka of infringing the copyright and the database rights of the newspapers. On its website, Eureka displays headlines in the form of a deep link. The court rejected all claims, saying it requires no substantial effort for a newspaper to compose a collection of headlines. Therefore Eureka does not infringe any database rights of the newspapers. The court also rejected the claim based on copyright infringement; it assumed that Eureka was a news agency, and according to article 15 of the Copyright Act, news agencies are allowed to copy articles.

These decisions demonstrate that, on the Internet, intellectual property rights can be invoked when a website provider uses third-party content on its website. It has to be said that certain terms such as 'substantial part' still need to be defined more accurately, and this will no doubt be done in case law.

With respect to the use of third party copyright protected music, the standard tariffs and contracts of the Netherlands collecting society Buma/Stemra should be mentioned. Buma/Stemra was one of the first collecting societies in Europe with Internet-related schemes. A distinction is made for different types of use of music on the Internet, including distribution of tracks (such as mp3-files), web-radio and web-TV, background-music on websites, web commercials, e-cards and ringtones.

Mention should also be made of the well-known *KaZaA* case, in which the Court of Appeals decided that by providing peer-to-peer software with which it is possible to

infringe third party copyrights KaZaA did not act unlawfully; it is also possible for end users to use the KaZaA software for non-infringing activities. International litigation is continuing.

20. *Can a website provider link to third-party websites without permission?*

Website providers are permitted to link to third-party websites provided they do not infringe third-party intellectual property rights or act unlawfully in any other way. The opinion has been advanced in Dutch literature, and even by the parties in the *NVM v De Telegraaf* case, that linking in itself does not constitute an infringement of third-party intellectual property rights nor an unlawful act, because it is a key element of the Internet, and third parties accept the key elements of the Internet when they publish their content on their websites. They thereby give an implicit permission to link to their content. This may be different when (framed) deep-linking is concerned. The above cannot be said if the third-party content is itself an unlawful use of other content. This was the situation in the *Scientology* case, the first on website linking related issues, and the following was decided: “By having a link on their computer systems, which when activated brings about the reproduction of the works that Scientology has the copyright to, on the screen of the user, without the consent of Scientology, the access providers (read: service providers) are acting unlawfully if and insofar they have been notified of this fact, the correctness of the notification cannot be reasonably doubted and the access providers (read: service providers) have then not proceeded to remove this link from their computer system at the earliest opportunity”. Other interesting linking related cases are *NVM v De Telegraaf* and the *Kranten.com* case mentioned above. Future amending legislation to the EU Copyright Directive may change the present situation as linking to copyright protected material may be considered making that material available to the public.

21. *Can a website provider exploit the software used for a website by licensing the software to third parties?*

A website provider can exploit the software used for a website by licensing, so long as the website provider owns the copyright with respect to the software. Otherwise, the website provider will need the prior permission of the copyright owner before licensing the software to others.

22. *Are any liabilities incurred by links to third-party websites?*

See 19 and 20 above.

23. *What legislation defines ‘personal data’ within the jurisdiction?*

Article 1a of the Personal Data Protection Act defines ‘personal data’ as any data concerning an identified or identifiable natural person. Legal responsibility ensues from the Act for those who control and who are able to influence the composition of a collection of personal data. The Telecommunications Act, which also contains privacy-related

provisions, makes a distinction between the privacy and personal data of subscribers, including legal persons, and of natural persons. The Telecommunications Act refers, with respect to the definition of personal data, in Article 11.2 to the applicable provisions in the Personal Data Protection Act; however, according to Article 11.5 personal data also consists of traffic data.

According to a detailed report of the Data Protection Authority on Internet privacy, personal data on the Internet can be divided in four categories: personal data which does not consist of data on Internet traffic, personal data which also consists of data on Internet traffic, traffic data on subscribers, and data on content.

24. *Does a website provider has to register with any controlling body in order to process personal data? Is it permissible for a website provider to sell personal data about website users to third parties?*

Under the Personal Data Protection Act, every registrar must notify the Data Protection Authority of its registration of personal data of any kind. Under present law, exceptions to this rule are made for relatively simple and frequently occurring registrations, such as subscription, salary and personnel administration. Such exceptions are regulated by the Exemption Decree PDPA of 7 May 2001. In most cases a website provider collects much more data than the data existing in simple registrations, and the website provider will thus have to register with the Data Protection Authority.

Personal data cannot normally be supplied to third parties. Exceptions to this general rule are supply to third parties on the basis of specific legislation, such as the provision of salary data on the basis of tax legislation, and where the individual concerned has given his/her explicit consent to the supply of personal data to a third party. There are many detailed rules to be followed before a transfer or sale of personal data to a third party can be made, which concern privacy statements, the methods by which data is collected and the specific method to be followed to secure explicit consent.

25. *If a website provider is intending to profile its customer base in order to target advertising on its website, is this regulated in your jurisdiction?*

There is no specific regulation in the Netherlands on whether a website provider is allowed to profile its customers in order to target advertising. There is also no case law on this, so general privacy rules will apply. As mentioned above, under the Personal Data Protection Act every registrar must notify the Data Protection Authority of its registration of personal data of any kind. It is expected that a registration by a website provider of the (traffic) profile of its customers, for instance by means of cookies, clicktrails, spiders, etc, is to be considered as a registration in accordance with the Personal Data Protection Act in the event such registration is being related to an individual. This generally has the consequence that the registration must be registered with the Data Protection Authority, that transfer of the registered data can only take place on limited conditions, that the consent of the data

subject is often required, and that the data subject has the right to adjust, remove or correct its registration.

26. *If an Internet company's server is located outside the jurisdiction, are any legal problems created when transferring and processing personal data?*

General rules with respect to the transfer of personal data to a server located outside the Netherlands for further processing are given in Articles 76-78 of the Personal Data Protection Act. According to these rules, a transfer to a non-EU country may in principle only take place when the country provides an adequate level of protection. The protection is judged with reference to all circumstances (in particular: the nature of the data, the intention of the transfer and the term of the intended processing of the data) influencing the transfer. The transfer to a non-EU country without an adequate protection regime is only possible in limited circumstances, provided the data subject has given unequivocal consent or the transfer is necessary for the conclusion or execution of an underlying agreement. By decree, it can be decided that transfers to these non-EU countries without an adequate protection regime are prohibited.

27. *Is it permissible to operate an online betting and/or gaming business from the jurisdiction?*

According to Dutch legislation on betting and gaming, only license holders appointed by the government are allowed to provide betting and gaming. Non-license holders providing betting and gaming are criminally liable. At present, there are nine license holders; the government's policy is to provide no additional licenses. The government's general approach to rules on the Internet ('what applies offline also applies online') also applies to betting and gaming: thus only license holders are allowed to provide online betting and gaming.

Since the mid-1990s, there have been several policy and discussion papers on the possibility to provide online betting and gaming. This has not lead to new legislation yet. However, it is the government's intention to make it possible to provide online gaming and betting in the future: the government has announced that some existing license holders will be allowed to provide online gaming and betting. In this respect, a Bill containing rules on online gaming and betting is currently under preparation.

In a recent court case, the UK gaming and betting provider Ladbrokes was ordered to cancel access for Dutch residents to its online gaming and betting website, which website was also aimed at Dutch clients. The reason for this was that Ladbrokes does not have Dutch license to provide gaming and betting to Dutch residents.

28. *Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?*

As mentioned in the previous question, the provision of online betting and gaming is at present not allowed under Dutch law. The participation in illegal betting and gaming is technically prohibited under the Betting and Gaming Act 1961. In practice there is no enforcement against Dutch individuals participating in foreign online gaming a betting websites. Several means of betting and gaming (such as casinos) are only available for individuals over the age of 18.

29. *What are the key legal issues relevant in considering the provision of services on an outsourced basis?*

As no specific legislation on outsourcing is available, normal contract law applies. Various practical and legal issues should be regulated, such as: a detailed Service Level Agreement (SLA); termination of the outsourcing agreement (including a transition period); hardware; deposit of data; the transfer or sublicensing of software; safeguarding trade secrets; and labor law.

30. *What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?*

Under Dutch legislation all employees, as well as the rights and obligations pertaining to them under their employment agreements, will automatically transfer with the outsourced business. All employees employed by the outsourced business will be able to enforce their rights vis-à-vis their new employer under their employment agreements. In the first year of outsourcing, the previous employer will be jointly and severally liable for all the obligations based on the period before the transfer. The new employer is not allowed to terminate the employment of the transferred employees merely on the basis that these employees were transferred as a result of the outsourcing. The above legal principle applies to all employees in the Netherlands.

31. *When would a website provider be liable for mistakes in information, which it provides online? Can it avoid that liability?*

In the Netherlands providing inaccurate information is not in itself sufficient to establish liability under tort law. However, a content provider should exercise due care as circumstances may require an accurate investigation. Negligence may provide sufficient grounds for liability under tort law. A number of factors are of importance for a court in determining the extent of the obligation to exercise due care, such as: the nature of the information provided (medical, political, personal, etc); the parties involved (eg a consumer); the interests involved; and other circumstances, such as whether the information is provided to a closed user group or to the general public. Obviously, in the event the information is provided to a closed user group whose subscribers have entered into an

agreement with the content provider, the content provider may also be liable under contract law, especially when the content provider is under an obligation to provide accurate information. Mistakes in online advertising may also result in liability under tort law when the advertisement is misleading. However, in principle this liability only applies between competitors. Finally, issues such as product liability and the conformity obligation in contractual relationships with consumers are also to be taken into account. Although information may not be considered as a 'good' or an 'object', these issues and corresponding legislation will probably have an effect on potential liability for mistakes in information.

Under Netherlands law a limitation of liability is generally allowed between companies but may be difficult to enforce with respect to consumers. Furthermore, a mere disclaimer on a website will in most cases not be sufficient. A limitation of liability of the content provider towards an end user of the content only applies when the end user has physically agreed with the terms and conditions of the disclaimer; physically clicking on a button is thus required. However, in the recent case of *Netwise v NTS* the District Court of Rotterdam ruled that in case of a professional end user a physical action of agreement with general terms and conditions with respect to the use of the website is not required under all circumstances.

32. *If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?*

If a database is the result of a substantial effort in terms of quality and quantity, the database will be protected under the Databases Act. Other people are then only allowed to reuse or reproduce substantial parts of the protected database with the prior permission of the database producer. Permission for reusing or reproducing minor parts of the protected database is not required. If a database producer wants to prevent other people from also reusing or reproducing minor parts of its database, it will have to prohibit such use in an agreement with the end user. This can be done in general terms of conditions or in a disclaimer placed on the website. Relevant cases dealing with reuse or reproduction of data from a protected database are *Netwise v NTS*, *NVM v De Telegraaf* and the *Kranten.com* case mentioned earlier.

33. *Is there any pending legislation, which is likely to have consequences for e-commerce and Internet-related issues?*

EU Directives relevant to e-commerce have been and will be implemented in the Netherlands as set out in the table on the following page.

EU DIRECTIVES	THE NETHERLANDS
Directive 1991/250/EEC of 14 May 1991 on the legal protection of computer programs, <i>OJ L 122/42</i> , 17.05.1991.	Act of 7 July 1994 to amend the Copyright Act 1912 in relation to the legal protection of computer programs, <i>Official Gazette</i> 1994, 521.
Directive 1993/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and related rights applicable to satellite broadcasting and cable retransmission, <i>OJ L 248/15</i> , 06.10.1993.	Act of 20 June 1996 to amend the Copyright Act 1912 and the Act on Neighboring Rights in relation to EU Directive 1993/83/EEC on the coordination of certain rules concerning copyright and related rights applicable to satellite broadcasting and cable retransmission, <i>Official Gazette</i> 1996, 364.
Directive 1993/98/EEC of 29 October 1993 on the harmonization of the term of protection of copyright and certain related rights, <i>OJ L 290/13</i> , 24.11.1993.	Act of 21 December 1995 to amend the Copyright Act 1912 and the Act on Neighboring Rights in relation to EU Directive 1993/98/EEC on the harmonization of the term of protection of copyright and certain related rights, <i>Official Gazette</i> 1995, 652.
Directive 1995/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <i>OJ L 281/31</i> , 23.11.1995.	Personal Data Protection Act of 6 June 2000, <i>Official Gazette</i> 2000, 302.
Directive 1996/9/EC of 11 March 1996 on the legal protection of databases, <i>OJ L 077/20</i> , 27.03.1996.	Act of 8 July 1999 to adapt Netherlands legislation to EU Directive 1996/9/EC on the legal protection of databases (Databases Act), <i>Official Gazette</i> 1999, 303.
Directive 1997/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts, <i>OJ L 144/19</i> , 04.06.1997.	Act of 21 December 2000 to adapt Book 7 of the Civil Code to EU Directive 1997/7/EC on the protection of consumers in respect of distance contracts, <i>Official Gazette</i> 2000, 617.
Directive 1997/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, <i>OJ L 024/1</i> , 30.01.1998.	Telecommunications Act of 15 December 1998, <i>Official Gazette</i> 1998, 610.
Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures, <i>OJ L 013/12</i> , 19.01.2000.	Amended legislative proposal to adapt Book 3 and Book 6 of the Civil Code, the Telecommunications Act and the Economic Offenses Act to EU Directive 1999/93/EC on a community framework for electronic signatures, <i>Parliamentary Documents First Chamber</i> 2001-2002, 27 743, no. 265.
Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, <i>OJ L 178/1</i> , 17.07.2000.	Amended legislative proposal to adapt the Civil Code, the Code of Civil Procedure, the Criminal Code and the Economic Offenses Act to EU Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market, <i>Parliamentary Documents Second Chamber</i> 2001-2002 / 2002-2003, 28 197, no. 1-2 / 6.
Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, <i>OJ L 167/10</i> , 22.06.2001.	Amended legislative proposal to adapt the Copyright Act 1912, the Act on Neighboring Rights and the Databases Act to EU Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society, <i>Parliamentary Documents Second Chamber</i> 2001-2002 / 2002-2003, 28 482, no. 1-2 / 6.
Directive 2002/58/EC of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector, <i>OJ L 201/37</i> , 31.07.2002.	No legislative proposal has yet been submitted.
Directive 2002/65/EC of 23 September 2002 on the distance marketing of consumer financial services, amending EU Directives 1990/619/EEC, 1997/7/EC and 1998/27/EC, <i>OJ L 271/16</i> , 09.10.2002.	No legislative proposal has yet been submitted.