

British Institute of International and Comparative law:
International Electronic Evidence

Edited by Stephen Mason (2008)

Chapter **Norway**, pp. 645-676+993:

*Harald Hjort and Svein Willassen*¹

A. THE LEGAL FRAMEWORK

Decisions made by judges should be based on a correct understanding of the relevant facts of the subject-matter before the court. The factual basis of a case must be proven before the court. The purpose of the rules of evidence is to provide guidance for the parties and the judges to reach a just legal conclusion in relation to the disputes they deal with.² In this respect, the rules of evidence are closely linked to fundamental principles of due process. These principles apply to both civil and criminal matters.

In Norway, both civil and criminal cases are generally handled by a uniform court system, applying general rules of procedure, one code for civil matters, The Disputes Act of 17 June 2005 (DA 2005),³ and one for criminal cases, The Criminal Procedure Act of 22 May 1981 (CPA).⁴

The civil procedure reform passed by the Norwegian Parliament (Stortinget) in 2005 was the result of extensive reports from a dedicated governmental legal committee.⁵ The reform also included a new Arbitration Act of 14 May 2004.⁶ The new DA 2005 entered into force on 1 January 2008, superseding the Disputes Act of 13 August 1915 (DA 1915).⁷

¹ The authors thank Professor Jon Bing, Norwegian Research Center for Computers and Law, University of Oslo, for reviewing this chapter.

² For an analysis of the basic principles of Norwegian evidence law, see eg Jo Hov, *Rettergang, Sivil- og straffeprosess* (Papinian, Oslo/Bergen, 1999) vol 1, 200ff.

³ Lov om mekling og rettergang i sivile tvister (tvisteloven) (17 June 2005) no 90. The details of the specific provisions of the Act are outlined in the commentary by T Schei, A Bårdsen, DB Nordén, C Reusch and TM Øye, *Tvisteloven—Kommentarutgave* (Universitetsforlaget, Oslo, 2007) vols 1 and 2, 1–1774. For a survey in the English language of the main features of Disputes Act 2005, see I Lorange Backer, 'The Norwegian Reform of Civil Procedure' (2007 51 *Scandinavian Studies in Law* 42–75).

⁴ Lov om rettergangsmåten i straffesaker (22 May 1981) no 25. For details about the CPA, see generally the commentary HK Bjerke and E Keiserud *Straffeprosessloven Kommentartutgave* (3rd edn, Universitetsforlaget, Oslo, 2001) vols 1 and 2, 1–1539.

⁵ NOU 2001:32 vol A and B *Rett på sak. Lov om tvisteløsning (tvisteloven)*, 1249 pages, with draft statute and summary in English. Chief Justice Tore Schei was chairman of the committee.

⁶ Lov om voldgift (14 May 2004) no 25, which entered into force 1 January 2005. The statute was based on a separate report NOU 2001:33 *Lov om voldgift (voldgiftsloven)* from the committee.

⁷ Lov om rettergangsmåten for tvistemål (tvistemålsloven) (13 August 1915) no 6.

Norway is a signatory to the European Convention on Human Rights (ECHR). Section 3 of the Human Rights Act of 21 May 1999,⁸ provides as follows: 'The provisions of the conventions and protocols mentioned in section 2 shall take precedence over any other legislative provisions that conflict with them.' In the event of a conflict between Norwegian domestic legislation and the international conventions relating to human rights set out in section 2, which included the ECHR, the international convention will prevail. Therefore, this convention, with its subsequent protocols and jurisprudence, has become an important source for Norwegian courts in defining the scope of several procedural rights, both in civil and criminal cases. Article 6 (1), which requires a right to a fair trial, is of special significance in this respect, but also other provisions of the convention and its protocols, such as Article 8 of the convention, securing the right to privacy, has had implications for the procedural rules of Norwegian courts.⁹

1. *Electronic Evidence and Procedural Codes*

Neither the DA 1915, the new DA 2005, nor the CPA contain specific regulation of electronic evidence. Accordingly, all legal questions relating to the search for, and the admissibility, presentation and evaluation of such evidence must be decided by the interpretation and application of the general rules of evidence set forth in the procedural codes.

(a) *Civil matters*

With respect to civil matters, the DA 1915 chapter 19 (sections 249–60) dealt with written evidence. The Norwegian Supreme Court generally assumed that these rules also applied to computer programmes, electronic archives and such like.¹⁰ In a dispute regarding access to email correspondence,¹¹ the court ruled that emails are considered to be 'written evidence'. In accordance with the provisions of section 237 of the DA 1915, the rules of disclosure of written evidence applied similarly to objects that serve the function of evidence. Consequently, there was, with respect to disclosure of evidence, generally no need to distinguish between documents and electronic evidence. This is consistent with the provisions of the new DA 2005, which defines 'real evidence' as opposed to 'testimonial evidence': in section 26-1 'real evidence' is defined as:

⁸ Lov om styrking av menneskerettighetenes stilling i norsk rett, (21 May 1999) no 30.

⁹ For a detailed review of the effect of the ECHR in Norwegian procedural law, see J Aall, *Rettergang og menneskerettigheter* (Universitetsforlaget, Oslo, 1995), E Møse, *Menneskerettigheter* (Cappelen, Oslo, 2002) and SE Jebens, *Menneskerettigheter i straffeprosessen* (Cappelen, Oslo, 2004).

¹⁰ [1987] Norsk Retstidende 420 ('Rt') (The Norwegian Supreme Court Reporter).

¹¹ [2004] Rt 1467.

individuals and objects (real property, movable property, documents, electronically stored information etc) who or which in themselves, or whose or which properties, states or contents, contain information which may be of importance to the factual basis for ruling on the case.¹²

(b) Criminal matters

In criminal cases, the CPA does not distinguish between written evidence and other types of evidence with respect to search and seizure. The provisions of section 203 of the Code provide that 'Objects that are deemed to be of significance as evidence may be seized until a legally enforceable judgment is passed. The same applies to objects that are deemed to be liable to confiscation or to a claim for surrender by an aggrieved person'. The Supreme Court has ruled that this may include computers and other electronic equipment, as well as digitally stored information as such.¹³ Further, the provision of section 210 of the CPA states that 'A court may order a possessor to surrender objects that are deemed to be significant as evidence if he is bound to testify in the case'. In response to this provision, the Supreme Court has admitted as evidence a telephone company's transcript of telephone calls made to and from a particular telephone number, in order to link the registered owner of the telephone to the crime.¹⁴

Moreover, the Stortinget has enacted additional provisions to the CPA dealing with the ability of the police to utilize new technology, including 'Concealed video surveillance and technological tracking',¹⁵ 'Audio surveillance and other control of communication apparatus (communication control)',¹⁶ and 'Other audio surveillance of conversations by technological means'.¹⁷ These provisions regulate the restrictions on the methods used by police during the investigation of criminal matters. The electronic evidence gathered from legitimate police work in accordance with these provisions is considered admissible.

2. The Right to Introduce and Present Evidence

The right to introduce and present evidence before a court is considered a fundamental principle of due process. This is now expressed in DA 2005 section 21-3 (1) with respect to civil cases: 'The parties shall be entitled to

¹² A detailed analysis of the issues relating to access to electronic evidence in civil matters under the new Disputes Act 2005, can be found in E Mosen, 'Bevistilgang til elektronisk lagret material' (2007) 13 *Tidsskrift for Forretningsjuss* 194-235.

¹³ [1992] Rt 904.

¹⁴ [1992] Rt 904; [1992] Rt 928; and [1997] Rt 470.

¹⁵ Chapter 15a, sections 202 a-202 c, amendment of 3 December 1999 no 82.

¹⁶ Chapter 16a, sections 216 a-216 k, amendment of 5 June 1992 no 52.

¹⁷ Chapter 16b, sections 216 l-216 m, amendment of 3 December 1999 no 82.

present such evidence as they wish. Exceptions to the entitlement to present evidence follow from sections 21-7 and 21-8, Chapter 22 and other rules of evidence in the statute.' Although the same concept is not expressed in the CPA, the Supreme Court has stated that the same right to introduce and present evidence applies with respect to criminal cases.¹⁸ This principle would, however, be in conflict with other fundamental values if it was applied unconditionally. As a result, there are a number of prohibitions and exemptions in place that require a judge to determine the case, sometimes without all the relevant information about the subject-matter.

3. Evidence Prohibitions and Exemptions¹⁹

(a) Statutory duty of confidentiality

For both civil and criminal cases, the legislation establishes a prohibition on presenting evidence that is subject to a statutory duty of confidentiality.²⁰ Evidence must not be presented if this cannot take place without the person in possession of such evidence breaching a statutory duty imposed on him as a consequence of his employment with such organizations as the government, a municipality, a supplier of postal services or telecommunication services or of obtaining access to a telecommunication network. However, the court has the discretion to hear the evidence:

After giving due consideration to the duty of secrecy, on the one hand, and to the clarification of the case, on the other, the court may decide that the evidence shall be given even though consent has been denied, or that evidence shall not be received even though the Ministry has consented. Before making such a decision, the court shall give the Ministry an opportunity to give an account of the reasons for its point of view. This account shall not be communicated to the parties.²¹

The Electronic Communications Act of 4 July 2003 no 83 (ECA), section 2-9, requires companies that install electronic telecommunications equipment and operators within the telecommunications business, to keep confidential any knowledge of the content of electronic communication in the

¹⁸ [1990] Rt 1008.

¹⁹ See generally J Hov, *Rettergang, Sivil- og straffeprosess* (Papinian, Oslo/Bergen, 1999) vol 1, 209-20.

²⁰ Disputes Act 1915 section 204 no 2; Disputes Act 2005 section 22-3 and Criminal Procedure Act section 118.

²¹ Disputes Act 1915 section 204 no 2, second paragraph, Criminal Procedure Act section 118, second paragraph. The provision is also found in Disputes Act 2005 section 22-3, however, with a different regulation with respect to the last sentence. Under this new provision, the Ministry's account shall be communicated to the parties.

networks they install or operate. An important exception is found in the third paragraph of the provision:

Despite the duty of confidentiality, information may be given to the prosecution authorities or the police about secret telephone numbers according to contract and other subscriber information, as well as electronic communication addresses. The same applies for testimonies before the court.

This statutory provision confirmed and codified previous Supreme Court rulings that telephone companies were required to release to the police subscriber data information about the use of an IP address.²²

(b) Confidences imparted to certain professionals

The prohibition also includes information imparted to those involved in certain occupations, including attorneys, physicians, clergymen and a number of other professionals.²³ For instance, the email correspondence between a client and his lawyer, or a patient's medical data may not be introduced as evidence, unless the client or the patient gives his or her consent. If privileged materials are accidentally put into the hands of the other side or a third party, which can happen very easily with digital data, such evidence should not be permitted. Correspondingly, the court should not allow a witness to testify about such privileged information that is not obtained properly. However, as discussed below, the courts will most probably resolve such issues of improperly obtained evidence by balancing the interests involved.

(c) Trade or business secrets

The legislation contains further rules limiting the right to obtain and introduce evidence. Of special significance is the exemption from presenting evidence relating to trade or business secrets. A party may refuse to testify or provide access to evidence that cannot be made available without revealing trade or business secrets. However, the court may, nevertheless, order that such evidence be made available, if, after balancing the relevant interest, it finds this to be required.²⁴ The term 'trade or business secrets' includes production methods and systems, know-how and market or financial information. In the digital environment, practically all such information within a company is stored electronically. To the extent such material is not excluded as evidence, it must generally be presented to the court as a paper transcript.

²² [1999] Rt 1944 and [2000] Rt 169.

²³ Disputes Act 1915 section 205; Disputes Act 2005 sec 22-5 and Criminal Procedure Act section 119.

²⁴ Disputes Act 1915 section 209, Disputes Act 2005 section 22-10 and Criminal Procedure Act section 124.

(d) Evidence obtained in an improper manner

Another general prohibition relates to evidence obtained in an improper manner. In the past, the law was based on precedents in civil and criminal cases, but the law in relation to civil proceedings is now codified in DA 2005 section 22-7, which states in a general manner: 'The court may in special circumstances refuse evidence that has been obtained in an improper manner.' In accordance with the principle of preventing the admission of evidence gathered illegally or in an unjustified way, the Supreme Court has previously denied the admission of recordings of telephone calls in a child custody case.²⁵ In this instance, telephone conversations between the children and their father were recorded by the mother. The members of the court considered the actions of the mother to be disloyal and offensive. This is not to say, however, that recordings of telephone conversations are inadmissible. Recordings of telephone conversations have been admitted into evidence, even when the recordings were made without consent, as in a civil contract dispute leading to a subsequent criminal case,²⁶ and a criminal case involving drug trafficking.²⁷

Other examples of the response taken by the Supreme Court with respect to this issue include a criminal prosecution involving charges for embezzlement, in which an employer covertly recorded employees at work on videotapes, because of a suspicion of theft.²⁸ The evidence of the recording was excluded as being improperly obtained. Similarly, in a civil case regarding claims of wrongful dismissal, the Supreme Court ruled that a covert videotape recording of the employee, allegedly showing theft from the cash register, was under the circumstances inadmissible as evidence.²⁹ In comparison, the Supreme Court decided that an employer, in another case of wrongful dismissal, was allowed to present as evidence business-related emails found in the employee's email inbox stored on the employer's computer system. This included emails revealing preparations by the employee in setting up a competing business.³⁰

Although these cases involved electronic evidence (recordings of telephone calls, videotapes, emails), the crucial question was not the nature of the evidence, but how it was obtained. New technology involving electronic equipment offers sophisticated means of securing evidence of other people's acts and behaviour, but when applied improperly, such evidence is likely to be excluded in a subsequent litigation. In the cases from the Supreme Court mentioned above, the court was especially concerned with the issue of a privacy challenge by virtue of the securing of the evidence. This is consis-

²⁵ [1997] Rt 795.

²⁷ [1999] Rt 193.

²⁹ [2001] Rt 668.

²⁶ [1981] Rt 377.

²⁸ [1991] Rt 616.

³⁰ [2002] Rt 1500.

tent with the ruling of the European Court of Human Rights in the case of *Copland v United Kingdom*.³¹ In this case, the employee's telephone, email and Internet usage were subjected to covert monitoring by the employer, allegedly in order to ascertain whether the employee was making excessive use of the employer's facilities for private purposes. The court found this was a violation of Article 8 of the Convention, establishing the right to privacy. The decision does not discuss the issue of admissibility of evidence obtained in violation of the Convention; however, it provides support for the view that such evidence would not be permitted under Norwegian law.

A related issue is the admissibility of the results of a polygraph test as evidence in Norwegian courts. Such evidence is also obtained by challenging the privacy of the witness or the accused. Due to such considerations, the Supreme Court has generally refused to admit such evidence,³² even though, as in the case cited, the evidence was obtained with consent and legally. In this instance, the disputed reliability of the evidence was an additional reason for the court's ruling.

4. Presentation of Evidence in Court

Norwegian District and Appellate Courts generally hear oral evidence, and the presentation of evidence is before the court adjudicating the issue.³³ The parties and the witnesses must in general appear before the court. In both civil and criminal cases, the court may nevertheless for practical reasons allow witnesses to testify over the telephone.³⁴ This has now become quite common. Documents and other written evidence must be presented orally, which generally requires the attorney to read the relevant parts of the evidence. Most often, however, the judge will accept a brief summary of a document, provided that the critical paragraphs and sentences are read. Information in electronic format is generally presented on paper as printouts.³⁵ There is no formal regulation ensuring the authenticity of such transcripts, neither in civil nor in criminal cases. If the magnitude or the nature of the data makes it inconvenient or impossible to present such material on paper in the usual way, the

³¹ *Copland v United Kingdom*, A 62617/00 [2007] ECHR 253.

³² [1996] Rt 1114.

³³ The Supreme Court, on the other hand, bases its decisions on written evidence. Only court-appointed expert witnesses may appear before the Supreme Court, Disputes Act 2005 sections 21-9 and 30-11 and Criminal Procedure Act section 340. Other witnesses are subject to deposition, that is, a judicial examination and the taking of evidence in a district court in accordance with the rules in the Disputes Act 2005 section 21-11 and chapter 27, and for criminal cases Criminal Procedure Act sections 338 and 270-1.

³⁴ Disputes Act 1915 section 199a, Disputes Act 2005 section 21-10 and Criminal Procedure Act section 109a.

³⁵ See eg [2001] Rt 1589, with description on pp 1594-5.

judge may appoint an expert to analyse and summarize the significance of the evidence.

Computer-generated animations and simulations may be permitted in court in both civil and criminal cases, but are rarely used. There are no specific provisions regulating to what extent such remedies may be introduced. General rules of evidence give the judge the option to reject any evidence if the relevant information or evidence should be presented in a different and more relevant, practical or efficient manner.³⁶ However, if such presentations are permitted, in order to convince the court, it is necessary to present or make available both the factual foundation and the underlying scientific or technical theory for the conclusion of the facts that the court is invited to draw.³⁷

5. The Role of Experts

In both civil and criminal cases, experts on the subject-matter, or the significance of the evidence, may play a role. The court may appoint additional expert lay judges when deemed necessary.³⁸ This may be relevant if the subject-matter of the case concerns information technology or the evaluation of electronic evidence. An example is in the famous 'DVD Jon case', where a boy named Jon, who was 15 years old, developed a computer programme which revealed the protected code used to prevent DVD films from being performed on unlicensed equipment. He distributed his programme for free on the Internet and was later charged for violations of the Criminal Code section 145 dealing with illegal access to or interfering with computer programmes. In the case, both the District Court and the Appellate Court appointed technical lay judges with special knowledge within computer science. He was acquitted.³⁹ In another example, two offshore mechanics working on an oil production platform were dismissed due to extensive downloading of pornography from the Internet to the employer's data system. A major issue was whether these activities implied a serious security risk or not. The Supreme Court appointed two experts on computer science. The judgment cites their differing views on the issue of

³⁶ Disputes Act 1915 section 189 no. 4, Disputes Act 2005 section 21-7 (2) c) and, somewhat modified, Criminal Procedure Act section 292.

³⁷ In the case reported in [2001] Rt 1589, involving a dismissal due to the employee's excessive use of the employer's internet and server capacity for private purposes, the parties attempted to present the nature and gravity of the issue with graphs and statistics. The court indicated (p 1595) that the underlying factual evidence was not satisfactory highlighted, and therefore the court was unable to draw certain conclusions from the material. However, the court upheld the dismissal.

³⁸ Disputes Act 1915 section 325, Disputes Act 2005 section 9-12 and Criminal Procedure Act section 277.

³⁹ [2004] Rettens Gang 414 ('RG') (Norwegian Contemporary Law Reporter).

security risk, but the court did not draw any specific conclusion in this respect. However, the employees prevailed.⁴⁰

Alternatively, or in addition, a technical expert may be appointed by the court for an analysis and assessment of the evidence, when this is found necessary for establishing a sound factual basis for ruling on the case.⁴¹ The parties may also make use of their own expert witnesses, without being appointed by the court. An illustration relating to digital evidence is the case concerning a number of employees of a company that resigned and set up a competing enterprise. The main issue was whether the individuals involved had illegally copied and subsequently taken advantage of access to large amounts of digitally stored information, including business correspondence and contracts with suppliers' agents and customers, financial and market information, as well as technical manuals and the source code of the company's electronic products.⁴² Before the Supreme Court, the procedural issue was whether a pre-trial taking of electronic evidence, which took place on the premises of the defendant with no prior warning, was carried out in accordance with the law. The Supreme Court quashed the Appellate Court's decision, which found the taking of the evidence unjustified, and referred the matter back to the District Court, which upheld its previous approval. During the proceedings, both parties made extensive use of expert witnesses. The Supreme Court noted that under the circumstances, it might be appropriate to have a court-appointed technical expert in addition, in order to filter the irrelevant and possibly privileged materials. During the process of preparing electronic evidence with the assistance of a court-appointed expert, the judge may have to resolve additional disputes as to the scope and admissibility of specific documents or parts of the material as evidence.

There are no formal requirements to be an expert witness in court. Anybody with knowledge, skills and experience that is considered satisfactory by the court may be appointed as an expert. If an expert is required, normally only one expert is appointed (for cost reasons), but it is also possible to have two or more experts appointed by the court. The court defines the assignment and gives the expert the necessary instructions, after having received comments and suggestions from the attorneys. The expert is required to examine the evidence and submit a written report. He is also obliged to attend the court hearing for the purpose of presenting his findings and considerations, and is subject to examination by the court and the attorneys. If the parties introduce their own expert witnesses, they are also

⁴⁰ [2005] Rt 51.

⁴¹ Disputes Act 1915 chapter 17, Disputes Act 2005 chapter 28 and Criminal Procedure Act chapter 11.

⁴² [2006] Rt 626.

permitted to attend the proceedings and ask questions of the parties, witnesses and other experts.

In civil matters, there were certain restrictions in DA 1915 section 197 regarding the presentation of written reports or statements from a witness, due to the principle of oral proceedings. However, these rules have been amended in DA 2005. The general principle of inadmissibility of written witness statements is now replaced by a somewhat more flexible standard.⁴³

6. The Taking of Evidence

In civil cases, written evidence is introduced to the proceedings as enclosures to the attorneys' preparatory briefs submitted to the court, in which the relevant witnesses are also identified. In their briefs, the attorneys indicate the relevance of a witness and other evidence: 'The party shall specify what the evidence is intended to establish, and shall briefly explain important information which will be provided by way of the evidence to the extent that such party cannot expect the opposite party to be aware of it.'⁴⁴ However, the detailed contents of the testimonies submitted by witnesses are not revealed until the oral hearing.

The court may order a pre-trial court meeting, whereby a witness is heard or other specific evidence may be secured. This typically takes the form of a judicial examination of a witness, who for various reasons (residing abroad, disability, sickness, age) is not obliged or probably not able to appear before the adjudicating court.⁴⁵ It is also possible that objects, including digitally stored information, may be secured by a pre-trial taking of evidence. When secured, the evidence must be presented to the adjudicating court as written evidence, or, if deemed necessary, in a report from a technical expert appointed by the court.

7. Evaluation of Evidence

Another basic procedural principle is the duty of the court to adjudicate on the basis of the free evaluation of the evidence. The evaluation of the evidence must be based on the facts that come to light before the court, and the findings of the court must form the basis for the ruling.⁴⁶ The same principle applies in criminal matters, although it is not expressed in the statute. There are no statutory provisions defining the relative weight of

⁴³ Disputes Act 2005 section 21-12.

⁴⁴ Disputes Act 2005 section 21-6 (2).

⁴⁵ Disputes Act 1915 section 267 and section 220ff, Disputes Act 2005 section 21-11 and chapter 27, and Criminal Procedure Act section 270.

⁴⁶ Disputes Act 1915 section 183, Disputes Act 2005 section 21-2.

electronic evidence when the judge, as the trier of fact, assesses such evidence in combination with the other evidence presented. Generally, there are no recordings of the testimonies presented to the adjudicating court. Therefore, in case of appeal, all the evidence must be presented once again to the Appellate Court, which has both the power and the duty to make its own assessment of the facts.

A judge does not apply legal presumptions considering the reliability of electronic evidence. The notions of 'real evidence' and 'best evidence', and the distinctions between direct and indirect evidence and primary and secondary evidence, have no legal implications for the judge in conducting the fact-finding process. The court, generally, must apply its sound judgment when determining the relevant facts, taking into consideration all evidence presented. This applies to both the District Courts as well as the Appellate Courts.

The Electronic Signatures Act of 15 June 2001 no 81 implements the EU Directive on Electronic Signatures,⁴⁷ and provides the legal framework for electronic communications. However, for the purpose of establishing the facts of a specific case, it has, in principle, no bearing whether the procedures of the Act have been followed or not.

8. Burden of Proof

A different issue from the evaluation of the evidence is the legal question of the burden of proof. In criminal matters, when determining the issue of guilt, the court applies the 'beyond reasonable doubt' standard, whilst in civil proceedings the 'general preponderance of the evidence' rule applies. These principles of burden of proof form part of the Norwegian customary law, and are not expressed in the procedural codes. Accordingly, there are no rules or general principles of burden of proof relating to electronic evidence in particular either.

9. Electronic Filing and Communications with the Court

Norwegian courts have established an electronic case-management system, but this is only for the internal use of the courts. No system for electronic filing and communications with the attorneys has been implemented to date. Attorneys may submit their briefs and documents to the court by email, but are requested to provide paper copies for the courts' paper-based archive system. When the law requires certain motions to be filed within a proscribed time limit, this can be done by email, providing paper copies are

⁴⁷ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, [2000] OJ L 13, 12.

also submitted simultaneously. Certain provisions are enacted as amendments to the Courts' Act of 13 August 1915 no 5 (section 146 and section 197a), delegating to the Government the power to issue regulations regarding electronic communication with the courts. However, no regulation has been issued. Thus, there is no current legislation as to email correspondence with the courts or the individual judges. Nevertheless, many judges and court officers informally exchange email correspondence with both attorneys and third parties.

10. *International Exchange of Electronic Evidence*

Norway has ratified the main international treaties on civil procedure.⁴⁸ Accordingly, parties to civil actions may obtain witness statements from other jurisdictions. Litigants in a foreign jurisdiction may request assistance from Norwegian courts in obtaining testimonies from individuals residing in Norway. The exchange of evidence may also include electronic evidence that can properly be taken where litigation or a prosecution is pending or likely. In criminal matters, electronic evidence may be obtained abroad through well-established international police cooperation and international conventions on mutual assistance in such matters.⁴⁹

B. CIVIL PROCEEDINGS

1. *Pre-trial*

(a) *The truthfulness requirement*

The right to introduce and present evidence in judicial proceedings is accompanied with a requirement that the parties contribute by providing an accurate and complete picture of the facts of the case. The provisions of section 21-4 of DA 2005 expressly require a general standard of truthfulness before the court. This was previously considered a part of the custom-

⁴⁸ This includes the Civil Procedure Convention of 1 March 1954, the Hague Convention on the Service abroad of Judicial and Extrajudicial Documents in Civil or Commercial matters of 15 November 1965, and the Hague Convention on the Taking of Evidence in Civil and Commercial Matters of 18 March 1970. For a survey of international conventions relating to civil procedure ratified by Norway, see booklet published by the Ministry of Justice: Justisdepartementet *Rundskriv G 04/2007 19 April 2007 Rettsanmodninger i sivile saker*.

⁴⁹ The Nordic Police Co-operation Agreement of 2 September 2002, The Europol, The Interpol, etc. See also the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Schengen Convention of 19 June 1990. For a survey of conventions relating to international cooperation in criminal matters ratified by Norway, see booklet published the Ministry of Justice: Justisdepartementet *Rundskriv G 19/2001 1 August 2001 Internasjonalt samarbeid i straffesaker—gjensidig hjelp i straffesaker og utlevering av loubrytere*.

ary law in civil matters, but has now been codified in the legislation. The parties are required to give the necessary explanations and summaries of evidence in order to fulfil this obligation. In addition, DA 2005 section 21-5 imposes an obligation on any person giving evidence in judicial proceedings to testify regarding the factual circumstances of a case, and to provide access to objects and such like that constitutes evidence in legal proceedings, subject to the limitations defined in detail in the statute.⁵⁰

(b) Obtaining evidence

Often, a litigant is not in possession of the relevant or crucial evidence. Such evidence may be in the possession of the opposite party or a third party. Despite the standard of truthfulness, it is considered to be of paramount concern that the litigants have efficient remedies for obtaining evidence if it is in the possession of the other side or a third party. The new DA 2005 expands the duties of both the parties and third parties to produce and provide access to evidence, compared to the now superseded DA 1915. In addition to the general principles laid down in DA 2005 sections 21-4 and 21-5, section 26-5 (1) requires that 'All persons are obliged to make available as evidence objects which are in their possession or of which they can obtain possession'. According to section 26-1, the term 'objects' include 'documents, electronically stored information, etc'. Furthermore, in order for the obligation in section 26-5 (1) to be implemented, section 26-5 (2) requires that both the parties and others may

... be ordered to answer questions as to whether they are aware of items of evidence and to undertake necessary investigations in such respect. They may also be ordered to prepare summaries, extracts or other descriptions of information which may be gathered from items of evidence.

Therefore, anyone in possession of digital information held on storage devices may be ordered to produce relevant printouts, and even to some extent edit or process such information, in order for the court to facilitate the understanding of the material. Alternatively, or in addition, the court may also demand access to the complete information, by ordering certain files on the computer be copied, or even demanding a mirror image of the relevant hard drives. This new provision may prove to be a practical response relating to dynamic digital data, such as financial accounts and sales statistics. However, section 26-5 (3) sets forth a limitation: the court may refuse access to such information if this

⁵⁰ The rules of evidence prohibitions and evidence exemptions are found in chapter 22 of the act. The exceptions for information covered by a statutory duty of confidentiality (section 22-3), confidences imparted in those involved in certain occupations (section 22-5) and trade and business secrets (section 22-10) seem to be the most relevant for electronic evidence.

... would incur expenses which are not reasonably proportionate to the dispute and the potential value of the evidence, or if the party has himself approximately the same possibilities for obtaining access to such evidence. The court may make access to evidence conditional upon the person having requested such access advancing the expenses involved.

These limitations apply in addition to the general restrictions on the entitlement to present evidence, including the principle of restrictions based on proportionality (section 21-8).

An application to obtain access to or questions concerning real evidence, such as electronically stored information, must be specified in such a manner that it is clear as to which item of evidence the application relates. The court may relax the specification requirements if they are considered to be unreasonable to comply with, provided that there is a clear possibility of the application providing access to the relevant evidence (section 26-6).⁵¹

In the event of a dispute concerning access to items of evidence, the court may demand that the item is submitted or presented to determine whether it constitutes evidence (section 26-7 (1)). If the application for access to evidence is met with an objection to the effect that this is subject to evidence prohibition or exemption, such items of evidence are not to be presented, unless the court, because of the authority vested in it by a specific statutory provision, determines that the evidence is presented (section 26-7 (2)). For instance, such provisions exist with respect to the statutory duty of confidentiality and business and trade secrets.⁵² If only a part of the item of evidence is subject to an evidence prohibition or exemption, the remainder can be presented if it is possible. Allegations that the evidence is privileged must be supported by a reason that may be proved. However, in the absence of other available evidence, it is sufficient that the party or witness substantiates this by way of an affirmation (section 26-7 (2), cf 24-8 (3)).

If a party fails to comply with a court order to submit or present evidence, this, of course, may easily affect the court's conclusion as to the facts of the case. The court may also, if the matter is considered to be of material importance to the other party, issue an order determining that a failure to reveal and release the evidence within a specified final time limit will constitute non-attendance in the case (section 16-7 (2)). If a person who is not a party refuses to comply with a legally enforceable interlocutory order on providing access to evidence, the court may issue a ruling that the order is subject to enforcement (section 26-8 (1)), which may eventually lead to a physical seizure of the evidence with the assistance of the law

⁵¹ For a general discussion of the scope of the right to obtain access to electronic evidence, including the specification requirement, see Monsen (n 12) 194ff.

⁵² Disputes Act 2005 sections 22-3 (3) and 22-10.

enforcement authorities. The same will apply to a party in cases where the court has a statutory duty to ensure a sound factual basis before issuing a ruling on the case (section 26-8 (2)), such as when material public interests are involved (sections 21-3 and 11-4). Failure to disclose evidence and tampering with evidence may also be considered a crime under the Courts' Act of 13 August 1915 no 5 chapter 10. As electronic evidence may easily be manipulated, such cases are likely to appear in the future.

(i) Email correspondence

As discussed above, in the case of [2002] Rt 1500, the members of the Supreme Court permitted the employer to present the employee's business-related emails in a wrongful dismissal case. The court found that the employer was justified in viewing the employee's email correspondence and other files, even though they are regulated by the Personal Data Act of 14 April 2000 no 31. The provisions of section 8(f) of the Act provided the justification for the employer to view the files. Generally, processing 'personal data', as defined in section 2, paragraph 1, requires a legal basis, and the employee's consent or a balancing of interests pursuant to section 8(f) is the most commonly applied legal basis for such viewing of an employee's email correspondence.⁵³ Guidelines from the Norwegian Data Inspectorate⁵⁴ enable the employer, because of its managerial prerogative, to determine that an employee may only use the employer's data-processing systems for job-related purposes. However, an employer may not reserve the right to read all email correspondence entering into or sent from the enterprise's system. One reason for this is that an employee cannot control what comes into his email box. Most employers find it acceptable that employees use the email system for certain private purposes. Most employees therefore use their employer's data-processing system for both job-related and private purposes. Accordingly, the question frequently arises whether an employer may check what an employee has done on the data-processing system, to whom he has written and what has been written. This type of problem usually arises when the employee is for some reason (such as illness or holiday) absent from work, and the employer may then have an objective need to check that no enquiries or orders are left unanswered; the employer suspects that an employee is acting disloyally—examples of this may be a suspicion that information is being passed on to competing

⁵³ Section 8 of the Personal Data Act requires that 'personal data' may only be processed if the data subject has consented thereto, or there is statutory authority for such processing, or the processing is necessary in order to (8(f)) '... enable the controller or third parties to whom the data are disclosed to protect a legitimate interest, except where such interest is overridden by the interests of the data subject'.

⁵⁴ The Norwegian Data Protection Agency, *E-mails and files* (3 January 2006), an English translation is available online at <http://www.datatilsynet.no/templates/Page___1358.aspx>.

companies; the employer suspects that an employee is acting in conflict with the enterprise's instructions and regulations or Norwegian law—an example is the forwarding of films with undesirable or illegal content as an attachment to an email. Violation of the Personal Data Act may, under section 48, be considered a criminal offence. There is therefore an obvious need for the enterprise to establish internal rules and guidelines for both the use of the data-processing system and for the employer's right to control such use.

The Data Inspectorate has published a draft regulation⁵⁵ based on the principle that the content of the email box belongs to the employee.⁵⁶ In accordance with this draft, the employer is only permitted to obtain access to the employee's email account with the consent of the employee, or in certain situations specified in the regulation. This includes the situation where the employee is absent for more than three days, or if there is a reason to believe that the employee is guilty of illegal or improper behaviour with respect to the use of email, or such behaviour can be proven by obtaining access to the email box.⁵⁷ In any event, the employer is required to follow certain procedures (and notify in advance to the extent possible) if the employer intends to open and read the employee's email correspondence, whether the correspondence appears to be business related or not.⁵⁸ The proposed regulation seems to be consistent with the recent *Copland* case⁵⁹ from the European Court of Human Rights, where the court found that the monitoring of the employee's use of the Internet and email amounted to a violation of Article 8 of the ECHR. However, it remains to be seen whether the proposed Norwegian regulation will enter into force.

Whether obtaining access to email correspondence is legal or not, and whether the content can be introduced as evidence in a subsequent litigation, remain different questions. As outlined above, the latter issue is dealt with in DA 2005 section 22-7, which provides that '[t]he court may in special circumstances refuse evidence that has been obtained in an improper manner.' Violation of specific regulations protecting privacy would typically constitute a reason for denying such evidence. In any event, the proposed regulation calls for employers to take appropriate measures, such as incorporating terms covering consent in future employment contracts and to provide instructions to employees with respect to the forwarding of email, the private use of email and the abuse of the email facilities.

⁵⁵ The Norwegian Data Protection Agency, *Proposal for new regulation of employer's access to employee's e-mails* (18 October 2006) available online in Norwegian at <http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/Horningsnotat_epost.pdf>.

⁵⁶ Draft regulation section 9-3.

⁵⁷ Draft regulation sections 9-4 and 9-5.

⁵⁸ Draft regulation section 9-7.

⁵⁹ *Copland v United Kingdom*, A 62617/00 [2007] ECHR 253.

An important element of the draft regulation is the right and duty to destroy email correspondence at the termination of the employment.⁶⁰ The proposed regulation may, therefore, act to limit the ability of a party to search for and provide relevant evidence to the court in a wide range of business-related cases. As it is commonplace for many people to use their office email addresses for private communications, deletion of emails may also affect the future possibilities for using electronic communication as evidence in private disputes, unless the employee has properly arranged for copies to be retained. Although the employees are protected against unwarranted access to their email communications, they nevertheless have the general obligation to contribute to the presentation of evidence according to the Disputes Act 2005, unless any prohibitions or exemptions apply. This is the case whether the employee is a litigant or a third party, as discussed above. However, this new regulation, if implemented fully, seems to have the capacity to create obstacles to the judicial process in obtaining relevant email correspondence for evidence purposes in both civil litigation and criminal proceedings.

(ii) The proportionality requirement

The DA 2005 section 21-8 introduces a new general limitation on the right to introduce and present evidence:

There shall be a reasonable degree of proportionality between the importance of the dispute and the scale and scope of the presentation of evidence. If the presentation goes beyond the limitations imposed by this requirement, the court may curtail such presentation of evidence to achieve the legislative intent pursuant to section 1-1, and within the confines of the restrictions resulting from such purpose.⁶¹

⁶⁰ Draft regulation section 9-6 deals with the access to emails after the termination of the employment: 'When the employment is terminated, the employee's personal e-mail box with the enterprise shall be closed and the content shall be deleted, unless otherwise is agreed in writing or is stated in regulations according to section 9-8'. Section 9-8 requires all employers to establish internal regulations for the employees' dealing with the email system. According to the definition in section 9-2, paragraph 1, the term 'personal e-mail box' include all emails to and from an email account defined by a name of an individual employed by the enterprise, eg john.doe@enterprise.com. Accordingly, all his business-related email correspondence is included.

⁶¹ Disputes Act 2005 section 1-1 defines the purposes of the act:

(1) The Act shall provide a basis for dealing with legal disputes in a fair, sound, swift and confidence inspiring manner through public proceedings before independent and impartial courts. The Act shall attend to individual dispute resolution needs as well as the need of society to have its law respected and clarified.

(2) In order for the purposes under (1) to be achieved:

—each party shall be permitted to argue its case and present evidence,
—each party shall be permitted access, as well as the opportunity to respond to the arguments and evidence of the opposite party,

This rule may become an obstacle for a litigant who intends to present extensive electronic evidence in support of his case. The search for and seizure of such evidence often involves costly technical expertise and subsequent time-consuming analysis. Clearly, evidence uncovered after an extensive search may constitute crucial evidence. However, there is a risk that the court might deny scrutiny of the defendant's computer with assistance of a court-appointed expert, if the plaintiff cannot convince the judge that this would lead to specific and important information that otherwise would not be available and this use of resources is in proportion with the significance of the case. What is proportionate is, of course, subject to the broad discretion of the court.

(c) Securing electronic evidence

(i) The legal remedy for securing electronic evidence

Electronic evidence may be lost during the ordinary use of a computer. For instance, the file metadata, such as the time the file was last opened, can be altered simply by opening a file. In some cases, such information can be important evidence. Generally, the more extensively the computer is in use, the higher the risk that information, including previously deleted material, can no longer be restored. Therefore, there might be a need to secure electronic evidence, even if the user may have no intention of tampering with the evidence.

Electronic evidence may easily be manipulated, removed or destroyed, which means it might be of vital importance to secure the evidence, even before litigation is begun. Where evidence is stored on a computer in the possession of the opposite party, it may be necessary to apply to a court for an order to secure relevant evidence without notification of the opposite party, should there be a risk that the evidence might be manipulated or destroyed once litigation has begun. In such a situation, the provisions set out in the Disputes Act 2005 section 28-3 offer a potentially powerful remedy: the court is authorized to issue a temporary ruling to secure evidence without notifying the opposite party, provided that there is a justifiable reason to fear that such notification could prevent the evidence from being secured.⁶²

—each party shall at one stage of the proceedings be permitted to argue its case orally, as well as to make a first-hand presentation of its evidence, before the court,

—the procedure and costs involved shall be in reasonable proportion to the importance of the case,

—grounds shall be given for important rulings, and

—rulings of special importance shall be open to review.'

⁶² Disputes Act 2005 section 28-3 (3) and (4) reads:

'(3) Evidence may be secured immediately provided that swift implementation is necessary to

The provisions relating to the securing of evidence are inserted into the statute in chapter 28, titled 'The securing of evidence outside a lawsuit'. This indicates that this particular remedy is not available once a lawsuit is filed. However, where litigation is pending, it may come to the attention of one of the parties that they fear evidence might be modified or destroyed, in which case an application can be made to secure evidence without notification, providing the applicant can demonstrate why such an application is deemed necessary. There are no precedents relating to the interpretation of this issue.

(ii) The background to the statutory provisions

The statutory provisions on the securing of evidence without notification of the opposite party have a rather short but uncommon history. In [2000] Rt 1261, a case involving the unauthorized use of computer programmes, the members of the Supreme Court generally ruled that there was no legal basis for requesting evidence to be secured before litigation is initiated. This appeared to be a troublesome legal position, given that Norway had ratified the TRIPS treaty.⁶³ This treaty requires that the judicial authorities of the Member States generally have the authority to order prompt and effective provisional measures to prevent an infringement of any intellectual property right from occurring, and to preserve relevant evidence in regard to the alleged infringement. The treaty also requires that the judicial authorities shall have the authority '... to adopt provisional measures without prior hearing of the other side where appropriate, in particular where any delay is likely to cause irreparable harm to the right holder, or where there is a demonstrable risk of evidence being destroyed'.⁶⁴ In [2000] Rt 1261, the Supreme Court failed to see that the treaty requires a remedy by which

secure the evidence. If possible, notification shall be given to the opposite party so he can be represented during the securing of evidence. If notice is not possible, the court shall appoint a representative for the opposite party, and shall as soon as possible inform the opposite party as to what has taken place.

(4) The court may make a temporary ruling for securing evidence without notification of the opposite party, provided that there is reason to fear that notifying the opposite party could prevent evidence from being secured. Neither the opposite party nor the public shall be informed until the securing of evidence has been implemented, or more than six months have passed since the matter is finalized. The person having submitted the application should not be allowed access to the evidence until the decision is final in circumstances where it may be of importance to the opposite party to prevent such access. Section 32-8 applies similarly. The time limit for application for oral hearing is two weeks from notification of the implementation.⁷

Section 32-8 deals with subsequent oral hearings where a court has ordered injunctive relief in favour of the plaintiff without an oral hearing, typically in urgent matters where a delay due to such a hearing might jeopardize the plaintiff's vital interests.

⁶³ Treaty on Trade-Related Aspects of Intellectual Property Rights. The TRIPS Agreement is Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco, on 15 April 1994. The treaty entered into force 1 January 1995.

⁶⁴ The TRIPS treaty Article 50, sections 1 and 2, (a) and (b).

a party may demand the securing of evidence without notifying the opposite party. Neither did the court discuss the implications of DA 1915 section 36 a, which states that the Act is to be applied with respect to the limitations in accordance with the international treaties ratified by Norway. Therefore, the Supreme Court's ruling in [2000] Rt 1261 appeared not to be in harmony with Norway's obligations under international law. In order to rectify this legal situation, and in order to satisfy the requirements of the TRIPS treaty Article 50, the Stortinget enacted an amendment in 2004, by adding a new section 271a to the DA 1915.⁶⁵ However, when this statutory right to a remedy for the securing of evidence was enacted, the scope was not limited to intellectual property rights, but extended to all civil claims.

The provisions appear to be particularly relevant to the securing of electronic evidence. This legislation, however, seems to be in need of modification. A number of practical questions of interpretation, especially as to how a court order is implemented, are not addressed in the statute, for which, see below. It is anticipated that the various unresolved issues will require the courts to interpret these provisions in the future.

(iii) The procedure of the court

The plaintiff must request a court order to secure evidence in possession of the other party or a third party. When making an application, the plaintiff must list the likely defendants in the subsequent litigation. The plaintiff should also present evidence as to the existence of the claim and the risk of involving the defendant in the securing of the evidence. If this basic requirement relating to the risk of notifying the defendant is met, the court may order the evidence be secured. The court may deny the plaintiff's request if the judge determines that the action is not proportionate, when taking into account the burden and costs involved, and the purported significance of the evidence. DA 2005 section 28-3 (4) requires that neither the public nor the defendant is to be informed of the action until the evidence is secured, or at the latest six months after the order is issued. This implies a duty of confidentiality upon the court and its staff.

Neither the provisions contained in section 271a of the DA 1915, nor section 28-3 of the DA 2005, provides for how the order is implemented where a judge issues such an order. If the court decides to permit an action to secure evidence without notification, obviously the matter is referred to the civil law enforcement authorities for implementation. As these authorities have neither the personnel with the necessary technical expertise nor the necessary tools to deal with the digital evidence, it is suggested that the

⁶⁵ Amendment to Disputes Act 1915 of 25 June 2004 no 49. When this Act was superseded by the Disputes Act 2005, these provisions of section 271a were replaced by the similar provisions in DA 2005 section 28-3.

court should appoint a technical expert and issue any necessary instructions. When such an expert is appointed, he would assist the civil law enforcement officers when entering the premises where the computers are assumed to be, in order to take control or possession of the evidence. This would normally be on the defendant's premises, but the evidence could also be located at the premises of a third party, such as where a company has outsourced its data systems and services.

With respect to the information that is to be provided by the plaintiff when applying for an order to secure evidence, it was held by the Supreme Court in the case reported in [2006] Rt 626, that it is not necessary to specify in detail in advance which documents and information are to be secured. However, after the evidence is secured, the material must be subject to further investigation and analysis. Since the court is not supposed to have the technical knowledge and equipment, nor the capacity to investigate huge amounts of data-stored information, this should be assigned to the court-appointed expert.

In the event that the defendant contests the lawfulness of the seizure of information without prior notification, the order itself is not subject to appeal. However, the defendant may, within two weeks from the notification of the implementation, request a hearing to review the order issued. If the defendant prevails, and the court that issued the order finds that the seizure was not justified, the plaintiff is liable for damages caused by the action. Alternatively, at the time of making the order, the court might also order the plaintiff to post a guarantee for costs and possible damages caused to the defendant as a consequence of the action.

(iv) The procedure for securing electronic evidence

It is paramount that electronic evidence is secured in a professional and proper way, in order to avoid subsequent disputes as to the integrity of the evidence. It must also be ensured that the evidence is complete and that the information on the computer remains unchanged. However, there are no formal regulations describing the procedure for securing electronic evidence in civil matters. The practical way of securing digital evidence is to arrange for a mirror image of the contents of the computers and hard drives. By this means, no specific search for or analysis of information on the computers is required on site. This procedure means that there is a minimum of interference with the legitimate business conducted by the defendant or the third party. However, depending on the circumstances, it may be sufficient to copy specific files, especially when the amount of potential material is vast and there are a large number of servers, indicating the need to limit the scope of the search on occasions.

The statute does not address the issue of who should assist, and who is allowed to be present during such an action. As indicated, in practical terms

the court must appoint an expert, and in some cases the court has even agreed that the plaintiff's technical expert may undertake the copying of the material. The members of the judiciary have yet to be requested to define the extent to which the plaintiff and its representatives should be allowed to be present or take part in the action to secure evidence in the possession of the defendant or a third party. Accordingly, it is left to the judge to provide for the necessary instructions to the civil law enforcement officer to make sure that the defendant's legitimate rights and interests are not abused during the process.

The statute also fails to define what means are considered available to the officer when carrying out a civil action to secure electronic evidence. As mentioned, DA 2005 section 26-5 (2) requires that both a party and a witness may be ordered to

... answer questions as to whether they are aware of items of evidence and to undertake necessary investigations in such respect. They may also be ordered to prepare summaries, extracts or other descriptions of information which may be gathered from items of evidence.

The detailed interpretation of this principle in relation to the seizure of electronic evidence is not clear. The provision deals with obtaining access to evidence during the preparation of a trial, and does not regulate the duty to cooperate before litigation is contemplated. In addition, this provision deals with the power of the judge, and is not directly applicable to the civil law enforcement officer implementing the judge's order to secure the evidence. During the securing action on site, it may not be an option for the officer to return to the judge for further instructions, since any interruption or delay could jeopardize the purpose of the operation. He is expected to complete his mission with the means available to him, although unexpected obstacles occur. Therefore, the civil officer in the field is left with some difficult legal issues of interpretation as to which means are justifiable in any given set of circumstances.

There are a number of unresolved practical issues relating to what the enforcement officer might actually do in order to obtain the evidence, and to what extent a defendant or a third party is required to assist. These issues include whether a person may be ordered to open his home or office, to unlock doors, to guide the way to the computers, to explain the nature or function of the hardware, the software or the stored information, to assist in the interpretation of information that can be viewed, to reveal a password, to give access to encrypted data or to instruct an administrator of the computer system to assist. Some general guidelines may be found in the Enforcement Act of 26 June 1992 no 86 sections 5-9 and 5-10. According to these provisions, the defendant has a duty 'to give the information which

is necessary for the enforcement'. To the extent deemed necessary, the enforcement officer may also 'claim access to a residence, business premises or other property, of which the defendant fully or in part owns or has possession'. If the enforcement is resisted, the officer may even 'apply proportionate coercive measures' and, if deemed necessary, 'require assistance from the police'. However, these provisions were enacted to ensure the efficient enforcement of civil claims. It remains uncertain as to what extent such measures can properly be applied for the purpose of securing evidence before litigation has been initiated and without prior notice to the defendant.

In the case reported in [2006] Rt 626, the Supreme Court generally stated that, subsequent to the securing of the material, the defendant may be required to assist in distinguishing the material, for instance by locating privileged documents to be excluded from the secured material, but there are no precedents as to the scope of available means in the securing of evidence outside legal proceedings that have already commenced. However, the prohibition on self-incrimination, as interpreted under the provisions of Article 6 (1) of the ECHR, should certainly limit the duty of defendants to actively assist during an action of securing electronic evidence on their computers initiated by the plaintiff.

(v) Subsequent access to and use of the evidence

There are no guidelines or regulations regarding who should take immediate possession of the material after it is secured, or how it should be handled. In practice, the civil enforcement officer responsible for carrying out the judge's order must take care of the material. DA 2005 section 28-3 (4) states that the plaintiff should not be given access to the material until the case relating to the evidence is decided, if it is considered important for the defendant to bar such access. This may be the case, for instance, if the material that is seized includes trade or business secrets and there is a risk of harm caused to the defendant if such information is revealed to the plaintiff. If there is no such apparent risk, the material that is seized could be handed over to the plaintiff for further scrutiny.

Some guidance was provided by the members of the Supreme Court in the case of [2006] Rt 626. It was assumed that the appointment of a technical expert is a practical method of having the electronic evidence analysed and assessed. The court noted that, at this stage, it could be appropriate to impose on the defendant certain duties to clarify which material is subject to investigation and which parts of the material could be regarded as privileged and therefore excluded. The court also noted that the purpose of the expert's investigation is to search for and scrutinize the material in order to locate relevant evidence. It is for the judge to define the requirements and give the necessary instructions. However, often a judge may not be in a position to issue any such detailed instructions or define the relevant search

criteria. This process of searching for possible relevant evidence within a large amount of digitally stored information may be a time-consuming task, which must be based on an understanding of the legal issues in dispute. From a practical point of view, an efficient search for the crucial and relevant evidence carried out by a court-appointed expert requires cooperation with the parties and their experts. It is for the judge to supervise this process. The expert's findings and considerations are to be presented in a report to the court, and the expert is also required to appear in court and be available for examination.

The taking of evidence by generally copying information found on the defendant's computer raises a number of issues relating to the information captured. Much of the information would most probably be irrelevant to the litigation. The material might also include information that is confidential and will be excluded as evidence. The statute does not address how the process of sorting the relevant material should be carried out whilst dealing with information that is confidential. It is a matter for the judge to decide on how to draw the line when defining the relevant and admissible evidence of the case, although this might require a careful consideration of the possible significance of a large number of files and documents.

(vi) Costs

The rules regarding the costs associated with the securing of evidence have not been decided conclusively. In general terms, where a plaintiff makes an application to the court for an order to secure evidence, he is liable for the costs of implementing the order (DA 2005 section 28-5). However, if the defendant disputes that the seizure of information was justified and requires a subsequent court hearing, it is possible that the general cost rules in DA 2005 chapter 20 apply. The main principle is that the successful party will have his costs reimbursed, but the court can make exceptions (DA 2005 section 20-5). There are no precedents defining the availability of these general cost rules to applications for securing evidence according to DA section 28-3.

C. CRIMINAL PROCEEDINGS

1. Pre-Trial

(a) Powers of investigation

The provisions for criminal procedure are set forth in the Criminal Procedure Act of 22 May 1981 no 25. Investigation of criminal matters is conducted by the police under the supervision of the prosecution authorities, comprising the public prosecutors and the lawyers employed by the police. The purpose of the investigation is to obtain the necessary information and evidence in order to decide whether to prosecute, to prevent or to

put a stop to criminal acts or activities, or to enforce a judgment. If there is an identified suspect, the police officers are required to search for information that is in favour of the suspect as well as information that is against him.⁶⁶ There are also special provisions in the Criminal Procedure Act for private criminal prosecutions (chapter 28). This option is, however, rarely used. The methods for obtaining electronic evidence in criminal investigations that are discussed in the following sections, such as disclosure, seizure and interception, are only available to the police and the prosecution.

(b) Disclosure of communication information

Disclosure of communication information is regulated by the Electronic Communications Act of 7 July 2003 no 83 (ECA).⁶⁷ The provisions of this statute address the requirements of providing electronic communication by means of infrastructure, services, equipment and installations (section 1-2). Providers are prohibited from disclosing the content and usage logs of electronic communications, pursuant to the confidentiality clause in section 2-9, subsection 1, of the ECA. Further, providers may not utilize such information in their own business, except where the information is in an anonymous form. Such information may only be disclosed when authorized by a statutory provision. An exemption is established in section 2-9, subsection 3, by which disclosure of information about a secret telephone number, other subscriber data or the use of an electronic communication address to the police or prosecution authorities is allowed. Such information can be disclosed to the police or the prosecution authorities without permission from a court. Representatives of the electronic communication provider may testify to the accuracy of such information.

The provisions outlined above are a continuation of the provisions contained in section 9-3 of the Telecommunications Act of 23 June 1995 no 39 (TCA), now superseded, in which regulations relating to the disclosure of data pertaining to the use of an electronic communication address were introduced in 1998.⁶⁸ Section 9-3 of the TCA was subject to several

⁶⁶ Criminal Procedure Act section 226.

⁶⁷ This legislation implements the following EU Directives: Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), [2002] OJ L 108, 7; Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), [2002] OJ L 108, 21; Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), [2002] OJ L 108, 33; Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), [2002] OJ L 108, 51.

⁶⁸ Amendment to the Criminal Procedure Act of 26 June 1998 no 53.

Supreme Court decisions in 1999 and 2000, regarding the disclosure of information relating to the use of an IP address on the Internet. In these cases, the police requested subscriber information from the Internet provider about an IP address at a specific moment of time, as identified by time stamps recorded on digital media when the IP address was used. The Internet providers contested that an IP address was considered an electronic communications address and argued that the police first would have to obtain a court order to collect such information. In its decision in [1999] Rt 1944, the Supreme Court ruled that subscriber data regarding the use of an IP address must be disclosed to the police, even if the IP address is dynamic, provided that the information can identify a particular subscriber. In the decision in the case reported in [2000] Rt 169, it was established that other information pertaining to the communication, such as the telephone number used to connect to the Internet, should also be disclosed when applying this procedure.

The disclosure of subscriber information to the police in criminal investigations without prior permission from a court has been firmly established by practice. This may include information about the user of an IP address or a telephone number, information about SIM numbers and telephone numbers that can be related to an IMEI number (identification of a mobile phone handset), email addresses and other types of information. Only subscriber information may be disclosed using this procedure. Records of an electronic communication itself can only be obtained through a court order, as discussed below.

(c) Data retention

In accordance with the provisions of section 2-8 of the ECA, providers of electronic communications are required to implement their service in such a way that makes it possible to obtain access to information about the communications that pass over the network. Subsection 3 of section 2-8 provides that the governmental authorities (the Norwegian Post and Telecommunications Authority) can issue regulations as to the provider's duties, such as the duty to retain data for a certain period of time. To date, no such regulations have been drafted. Following the passing of Directive 2006/24/EC,⁶⁹ such provisions are likely to be issued in the near future.

In order to comply with the provisions of Article 16 of the Council of Europe Convention on Cybercrime,⁷⁰ a provision for the expedited preser-

⁶⁹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105, 54.

⁷⁰ Budapest (23 November 2001).

vation of data was introduced in section 215a of the CPA in 2005.⁷¹ This additional section has incorporated the provisions of Article 16 into domestic law. Pursuant to this provision, the prosecution authorities may, during an investigation of criminal matters, instruct those who possess digital data, which may serve the function of evidence, to preserve them for a specified period of time. The preservation order must be rendered by the prosecution authorities and does not require court approval. The preservation period is not to be longer than considered necessary, and in any event, no longer than 90 days. If the order is issued as the result of a request from the authorities of a foreign country, the period is at least 60 days. The provision for data preservation applies to any person or organization that is in possession of digital data, not only to electronic communication providers. The data preservation provision can therefore be applied in any criminal case involving electronic evidence. A request for data preservation must pertain to data already stored at the time of the request. The prosecution may not issue a data-storing order. Any request pertaining to future communications must be issued according to the procedure for lawful interception.

(d) Search and seizure

The general provisions for search and seizure are provided for in chapters 15 and 16 of the CPA. A search may be carried out when there is probable cause for suspicion that the suspect committed an offence that might result in imprisonment. The suspect's residence, room or storage area may be inspected and searched for evidence or objects that may be seized. Searches can also be carried out on the premises of a third party if the offence was committed there, the suspect was apprehended there, or if there is any other specific reason to believe that there is evidence or objects to be seized there.⁷²

Before conducting a search, a search order must be obtained from a court in accordance with the provisions of section 197. There are several exceptions to this rule, such as if it is urgent or if the suspect is caught in the process of committing an illegal act. During the search, the police officer can seize any object that is believed to be of significance as evidence. The owner of the object may contest the seizure before the court. The seizure provisions apply to any object, including documents and devices containing digital data. The police may therefore seize any computer, hard drive, mobile telephone or other digital storage medium during a search, even when the search is conducted at the premises of somebody other than

⁷¹ Amendment to the Criminal Procedure Act of 8 April 2005 no 16.

⁷² Criminal Procedure Act section 192.

the suspect, or when the object is owned by someone other than the suspect. The principle of proportionality applies for search and seizure.

Thus, storage media containing digital data can be seized. Whether digital data itself can be seized, without seizing the actual medium, for example by copying the data, was considered by the Supreme Court in [1992] Rt 904. The court ruled that making a transcript of a list of telephone calls made from a specific telephone number within a specified period of time was within the scope of section 203 of the CPA. For this reason, it is at the discretion of the police officer carrying out the search whether to seize the actual storage medium or only the information stored within the system. With current methods for digital forensic analysis, it is possible to make a mirror-image copy of data stored on digital media without any loss of information. Applying the principle of proportionality, the police will, in most cases, seize the physical object itself only if it belongs to the suspect. As discussed in relation to civil matters above, it is paramount that the evidence is secured professionally and properly, in order to obtain a complete version of the material, which can be defended on technical grounds. However, there are no formal regulations describing the procedure for the police when securing electronic evidence.

According to the provisions of CPA section 210, the court may order the person in possession of an object that appears to be of significance as evidence to provide it to the prosecution. This is particularly relevant in cases where a third party retains or stores data on behalf of a suspect, for example if the suspect has stored data on a computer owned by a provider. Under such circumstances, it is not necessary for the police to carry out a search at the premises where the data is kept. The requirements for such an order are similar to the requirements for conducting a search.

The provisions of section 211 of the CPA permit the seizure of letters, telegrams and other communications kept by a postal operator or provider of electronic communication as part of a service conveying such objects and communication. Seizure is only permitted if it could legally take place from the final recipient and if the act is punishable pursuant to statute by imprisonment for a term exceeding six months. However, according to CPA section 212, communications seized in this way may only be opened and read by the judge, unless the sender consents in writing. In the absence of any provision to the contrary, it must be assumed that these provisions only apply to emails or other correspondence stored by the provider at the time of the seizure, otherwise large amounts of relevant evidence could not be seized legitimately. It is presently unclear how the provisions for seizure relate to the various forms of information stored on the provider's computer that may not necessarily be construed as correspondence or communication. It is also uncertain whether the provisions apply when the suspect has actually received the information, but it is still stored on the

provider's computer. The present practice is that the police examine emails stored on a computer that has been seized and which belongs to the suspect without submitting the individual emails to the judge for examination.

During a search involving computer systems, the police may face practical difficulties in obtaining access to the information. For example, the computer system may be protected by a password or it may contain encrypted data. It may also be the case that the computer system is of a type that requires assistance from a system administrator. These difficulties were recognized and addressed in Article 19 of the Convention on Cybercrime, and implemented in 2005 by the addition of section 199a to the CPA.⁷³ Pursuant to this provision, the police may instruct anyone who has knowledge of the computer system to assist them in order to obtain access to the system. Failure to provide such assistance is punishable by the imposition of a fine.⁷⁴ The suspect is exempted from this duty to assist, due to the prohibition on self-incrimination based on the provision of Article 6 (1) of the ECHR.

(e) Lawful interception

The legal basis for the interception of communications is provided for in chapter 16a of the CPA. According to the provisions of section 216a, lawful interception may only be implemented during investigation of specific offences. All offences that might result in more than 10 years' imprisonment are included, such as homicide, sabotage, terrorism, violent crimes and certain drug offences. Common types of financial crime and computer crime are not included. In addition, several specific crimes relating to national security may justify legal interception. Generally, interception requires a court order. One exception is where the prosecuting authorities fear that the outcome of an investigation may be endangered if it was necessary to await a court order. In such circumstances, the prosecuting authority may legally begin to intercept, but the decision must be submitted for approval by a court as soon as possible, and not later than 24 hours after the interception was initiated.

Lawful interception is conducted by audio surveillance of telephone calls or other methods of communication to and from specific computers, telephones or equipment for electronic communications used by the suspect, or methods of communication that it reasonably can be assumed that the suspect might use. The interception order can be served upon whomsoever owns the communication infrastructure. The owner or operator of such

⁷³ Amendment to the Criminal Procedure Act of 8 April 2005 no 16.

⁷⁴ Criminal Procedure Act section 199a, with reference to the Penal Code of 22 May 1902 section 399 no 1.

equipment may be instructed by the police to provide the necessary assistance.

In accordance with the provisions of CPA 216c, there are several additional requirements that must be met in order to obtain a court order for lawful interception. First, interception is only permitted if it can be assumed that the evidence obtained will be of relevance to the case under investigation, and that the investigation otherwise would be hindered considerably. Secondly, if the suspect's telephone or computer is regularly used by others, or if it belongs to certain professionals, including attorneys, doctors and clergymen, the prosecuting authorities are required to provide reasons to demonstrate why interception is necessary. Such a reason could, for example, be that the telephone or computer in question is known to be used regularly by the suspect for communication regarding the matters under investigation. A court order for the interception of communications may be rendered for a period of four weeks only; hence the prosecution must obtain a new order should it wish to continue the interception after the four weeks.

All types of data may be intercepted, including telephone conversations, emails, login sessions, web surfing, peer-to-peer traffic and other data. New communication technologies have, however, caused certain practical challenges. The interception of certain communication infrastructures may require advanced knowledge and technical support. In Norway, these challenges are addressed by the integration of the National Computer Crime Investigation Unit into the Norwegian Criminal Investigation Service (NCIS) in 2004 and the recent establishment, in 2007, of a national unit for lawful interception within the NCIS. Data specialists are employed in this Unit, and it serves as the national competence centre within the field of lawful interception of data and telephone communication. The unit conducts interception of electronic data at the request of regional prosecution officers.

(f) Seizure of communication records

The seizure of communication records is dealt with in CPA section 216b, subsection 2 (c). Communication records are defined as information about which communication entities have been or are to be put in contact with other communication entities during a specified period of time, and other data pertaining to such communication. Typical examples of such data include Call Detail Records from telephone networks, logs from email servers and other logs from communication networks. The providers of such communication services may be ordered by the court to provide such information to the prosecution when there is probable cause of suspicion of certain criminal activities. This includes all offences that, pursuant to statute, may result in five years or more of imprisonment, and certain spec-

ified offences relating to national security, computer intrusion and possession and production of child pornography.

(g) Disclosure

During a criminal investigation, the investigation documents are generally, upon request, made available to the suspect and his counsel, if disclosure can be made without endangering the purpose of the investigation (CPA section 242). When the suspect is indicted, the prosecution must disclose all documents to be presented as evidence in court, in accordance with the provisions of section 264. Defence counsel may not be denied access to such documents. Generally, defence counsel also has access to all other investigation documents, including materials upon which the prosecution does not intend to rely. Defence counsel may, however, be denied access to documents which are not intended to be utilized as evidence, when there is a risk that disclosure may result in violent crime, severe obstruction of the investigation or unwarranted disclosure of police methods. Decisions to deny disclosure on these grounds require a court order, on petition by the prosecution. Any denial of disclosure of investigation documents may be presented to the court by defence counsel.

Whether the defence is entitled to have complete copies of digital data seized during an investigation was subject-matter in a Supreme Court ruling in [2006] Rt 1193. In this case, the defence counsel requested a complete copy of all the electronic material that was seized in order to engage an independent expert to perform a search throughout the material for additional evidence. The prosecution argued that the defence and its expert should only be given access to the data within police premises, in order to maintain data protection and security. In its decision, the Supreme Court ruled that the data that was seized was to be considered part of the investigation documents, and therefore must be made available to the defence counsel. This should be made by submission of a complete electronic copy of the material, enabling the defence to arrange for further scrutiny. There are no regulations to ensure that the material is properly safeguarded. In this case, it was an issue that the material appeared to be the property of a third party. The court noted that such issues must be resolved by prohibitions on the use of the material for purposes other than defending the accused.

2. International Police Cooperation and Exchange of Evidence

The international exchange of information relating to criminal matters may take place directly between the domestic police and prosecution and their opposite numbers in a foreign country, without the need to implement procedures before a court for international assistance.

The CPA imposes a duty of confidentiality on public officials taking part in criminal investigation and prosecution; section 61c lists a number of exceptions where the duty of confidentiality does not apply. These include the use of information to fulfil the purpose of the investigation, and provision of information to other authorities to prevent criminal activities. These provisions do not distinguish between domestic and foreign authorities. Therefore, it is generally held that the Norwegian police may provide evidence directly to the prosecution in another country or through police cooperation organizations, such as Interpol. The direct exchange of evidence enables the law-enforcement authorities to speed up investigations where several countries are involved, such as crimes involving use of the Internet.

The current practice is that evidence that has not been obtained by court order can be exchanged directly through police cooperation. Evidence that has been, or must be, obtained by court order must be submitted under judicial procedures. Further to the discussion above, this means, for example, that subscriber information pertaining to the use of an IP address can be exchanged through police cooperation, whereas a list containing the details of the records of telephone calls must be disclosed by court order following a letter rogatory from the foreign country involved.

In cases involving a complaint where the suspect is believed to reside in another country, the Norwegian police authorities would usually submit the investigation documents directly to their opposite number in the particular foreign country, with a request to investigate and prosecute the suspect. Similarly, if police authorities in another country have reason to believe that the suspect resides in Norway, they would submit the matter to Norway, if permitted by domestic law, with a request for further investigation and prosecution. In such a case, the Norwegian police are generally required to adhere to the provisions of the Criminal Procedure Act, including rules relating to the search for and the admissibility of electronic evidence.

3. Data Protection in Criminal Proceedings

Privacy concerns, as reflected in the Personal Data Act of 14 April 2000 (PDA), have less relevance for the admissibility of evidence obtained in criminal investigations, compared to civil proceedings. Section 8 of the PDA lists the conditions for the processing of personal data when the data subject, that is the person involved, has not consented. This includes the processing of personal data in accordance with the statutory provisions and the proper exercise of government powers. Since the police investigation and prosecution is an exercise of such a public authority, the obtaining and processing of personal data searched for or the presentation of evidence is within the scope of PDA section 8. Electronic evidence obtained through criminal proceedings is therefore seldom contested on grounds of the PDA.

NORWAY

- Backer, IL, 'The Norwegian Reform of Civil Procedure' (2007) 51 *Scandinavian Studies in Law* 42–75.
- Bjerke, HK and Keiserud, E, *Straffeprosessloven kommentarutgave* (3rd edn, Universitetsforlaget, Oslo, 2001).
- Datakriminalitet*. Økokrims skriftserie no 9 (1995).
- Datateknikk og samfunnets sårbarhet*, NOU 1986:12 (1986).
- Hov, J, *Rettergang, Sivil- og straffeprosess*, vol 1 (Papinian, Oslo/Bergen, 1999),
- Justisdepartementet, *Internasjonalt samarbeid i straffesaker – gjensidig hjelp i straffesaker og utlevering av lovbrytere*, Rundskriv G 19/2001, 1 August 2001
- Justisdepartementet, *Rettsanmodninger i sivile saker*, Rundskriv G 04/2007, 19 April 2007.
- Lovtiltak mot datakriminalitet—Delutredning I*, NOU 2003:27 (2003).
- Lovtiltak mot datakriminalitet—Delutredning II*, NOU 2007:7 (2007).
- Monsen, E, 'Bevistilgang til elektronisk lagret material' (2007) 3 *Tidsskrift for Forretningsjus* 194–235.
- Rett på sak. Lov om tvisteløsning (tvisteloven)*, with draft statute and summary in English, NOU 2001:32 vols A and B.
- Edvin, J and Skoghøy, A, *Tvistemål*, (2nd edn, Universitetsforlaget, Oslo, 2001).
- Sunde, IM, *Lov og rett i cyberspace* (Fagbokforlaget, Bergen, 2006).

Norway

Harald Hjort has a *candidatus juris* (degree) (1983) from the University of Oslo and an LLM (1985) from the University of California, Berkeley. Since 1988 he has been a partner in the Hjort Law Office in Oslo, and in 1994 he was admitted to appear before the Supreme Court. Hjort is head of the law firm's litigation department. As an attorney-at-law, Harald Hjort appears regularly before the ordinary courts and arbitration courts in a wide range of cases.

Svein Y. Willassen has an MSc in information security from the Norwegian University of Technology and Science. After graduation, Willassen was employed as a special investigator at the National Computer Crime Center in Norway and as an investigation manager at Ibas AS, where he conducted a large number of computer forensic examinations in Europe and elsewhere in Scandinavia. Willassen is currently working on a PhD on digital evidence at the Norwegian University of Science and Technology. He lectures regularly and is an independent expert on digital forensics and evidence.