



Oslo First Instance Court¹

May be published

7 January 2003 there were pleadings before the court in Oslo Court House to make a

SENTENCE

President of the court: Assistant judge *Irene Sogn* with general authority
Expert co-judges: *Terje Knudsen*, Senior engineer
Stein Marthinsen, College lecturer

Case no: 02-507 M/94

The public prosecution

Counsel: *Inger Marie Sunde*, senior counsel for the prosecution

Vs

Jon Lech Johansen, born 18 November 1983

Counsel for the defence: *Halvor Manshaus*, Attorney-at-law

ABSTRACT OF THE JUDGEMENT FOR LOVDATA² FOR CASES CLASS M

Abstract: Criminal law. The penal code section 145 second paragraph cf. third and fourth paragraph. A 19 year old man was indicted for violation of the penal code section 145 second paragraph cf. third and fourth paragraph. He had developed a computer program making it possible to view DVD-movies without licensed playing equipment. The court found first that access to movies legally purchased was not unlawful with respect to the penal code section 145 second paragraph even if the movies were viewed in a different way than presumed by the producer. Second, the court found that disclosure of encryption keys by itself did not constitute unauthorised access to data. Nor could the indicted be convicted as an accomplice to the possible unauthorised access by others to DVD-movies because the program also had a

¹ Unofficial translation by Professor Dr. Juris. Jon Bing, Norwegian Research Center for Computers and Law, Faculty of Law, University of Oslo (jon.bing@jus.uio.no). The Norwegian language original is available at the Oslo Court's official web site <http://www.domstol.no/archive/OsloTingrett/Nye%20avgjorelser/DVD-jon.doc> or from Lovdata, PO Box 41 Sentrum, NO-0101 Oslo, Norway. The footnotes are the translator's.

² Lovdata is the computerised national legal information service of Norway, the abstract is authored by the judge.

legal application. After discussions and voting behind closed doors, there was in public given the following

sentence:

Jon Lech Johansen, born 18 November 1983, lives in Agmund Bolts vei 62. He is unmarried and has no children. He works as program developer and has a gross income of 35 000 NOK monthly. He has no estate.

By indictment of Økokrim³ state prosecutor's office of 10 May 2002, amended at the main hearing, he has been indicted before Oslo first instance court for violation of

Criminal code section 145 second and fourth paragraph

By breaking a protection or similarly gaining access to data stored or communicated by electronic or other technical means, and having caused damage by availing himself of or use of such unauthorised knowledge or having co-operated in this.⁴

The basis are the following facts, or co-operation in these

In the period September 1999 – 24 January 2000, through the Internet from his domicile in Lardal, *Jon Lech Johansen* co-operated in breaking the technical protection system Content Scrambling System ("CSS"), licensed by the *DVD Copy Control Association Inc*, to protect DVD-movies produced by *Motion Pictures Association* for copying. A DVD-movie is a movie stored electronically on a DVD-disk. Based on knowledge of a secret algorithm and playing keys incorporated by CSS, *Jon Lech Johansen* developed the Windows program DeCSS. By using DeCSS, a non-protected copy of the movie is produced, and he distributed DeCSS several times in several versions through the Internet in this period. Through the events described, *Jon Lech Johansen* gained unauthorised access to the secret key storage in CSS. Further, *Jon Lech Johansen* broke the copy protection of the DVD-movies making available for him and others the DVD-disk in unprotected form. The access was unauthorised because the DVD-movie was sold on the condition that the user should have authorised playing equipment and respect the copy protection. Making the movies available in unprotected form has caused damage as the right holders no longer has protection against unauthorised distribution of the movies.

The main hearing was in Oslo Court House 9 to 16 December 2002. The indicted met with his attorney. The indicted explained himself and declared himself not guilty according to the indictment.

The court heard five witnesses, and there was made such documentation as recorded in the protocol. Also the program DeCSS was demonstrated.

The counsel for the prosecution requested the court to make the following sentence:

³ Special central division of the public prosecutor for economic and similar types of crime.

⁴ Citing the relevant provision.

1. *Jon Lech Johansen*, born 181183, is sentenced according to the indictment to a punishment of prison in 90 – ninety – days, which are made conditional with a trial period of 2 – two – years, cf. the penal code sections 52 and following.
2. *Jon Lech Johansen*, born 181183, is sentenced to suffer the seizure of
 - One PC-cabinet Pentium III 500 MHz (seizure A-2), cf. the penal code section 35 second paragraph.
 - 8 CD-ROMs containing assorted unlicensed software (seizure A-4-6), cf. the penal code section 35 second paragraph.
3. *John Lech Johansen*, born 181183, is sentenced to bear the full costs of the case with 10,000 – ten thousand – NOK.

The counsel of the defence requested the court to make the following sentence:

Jon Lech Johansen is acquitted.

Comments by the court.

The basis of the case.

Bearing in mind the strict claims for proof in criminal cases, including the rule that any reasonable doubt should count in favour of the indicted, the court finds the following facts proven:

4 January 2000 the *Motion Pictures Association* (hereafter referred to as MPA) and *DVD Copy Control Association, Inc* (hereafter referred to as DVD CCA) reported *Jon Lech Johansen* to Økokrim for violating the penal code section 143 second paragraph. The basis of the report was that *Johansen* had taken part in the development of the computer program DeCSS.

MPA comprises several large American movie companies. The organisation was one of those taking the initiative which led to the founding of DVD CCA. DVD CCA was founded to stop piracy copying of DVD-movies. The DVD technology is described in the expert report prepared by Stig Frode Mjøl̄snes and Håkon Styri 18 September 2000 on request by Økokrim. From the report page 6 is cited:

“DVD is a further technological development of the compact disk (CD-disk), and has the same physical measurements [dimensions] as it. The storage capacity of a DVD is considerably larger than for the compact disk. DVD is used as a digital storage medium both within the entertainment industry (music, video, games) and computer industry (software, data bases *etc*). “

From the report page 7 is cited:

“DVD-Video is an ‘application’ of a DVD-ROM presuming among other things that the information on the disk is structured in a certain way.”

John Hoy, president of the DVD CCA, explained during the main hearing that as a DVD-video is based on a technology for storing information in digital rather than analogue form, the content may be copied without loss of quality. The movie companies were therefore concerned that the development of the DVD-technology would lead to a considerable number of disks being reproduced and distributed without the producers of the movies receiving any payment. He explained further that the companies backing the development of the DVD-technology wanted the co-operation of the movie industry in order to having something to sell. A compromise between the movie producers and the DVD-producers was the

development of Content Scrambling System (hereafter referred to as CSS). Asked by the counsel for the prosecution, Hoy confirmed that the development of CSS was a consequence of requests from the movie industry.

From the report by Mjøl̄snes and Styri page 13 is cited:

“CSS is a technological solution using cryptography to protect digital information stored on a DVD disk in accordance with[?] the DVD-video standard.”

The court bases its argument on this explanation of CSS.

From the report by Mjøl̄snes and Styri page 15 and 16 is cited:

“The fundamental problem a rightholder and publisher of a copyrighted work is confronting is how to control their intellectual rights at the same time as copies of the work are being distributed ...

By distributing a work in encrypted form the publisher will limit the dissemination of the work to those who knows the decryption key ...

One could attempt making a technological protection which would prevent the receiver from making the key available to others. This copy protection of decryption keys is a central element of CSS. Even so, this would not be sufficient. The receiver has an obvious and legitimate claim to use (see and hear) the content. Therefore, it is also necessary to prevent technological copying of the content after it is decrypted and is available as a ‘clear text’.

A common solution for this is to make the user dependent upon a *decoder and displayer* to see and hear the digital content. A condition which will have to be satisfied, is that there is no way of ‘tapping’ the displayer of the content being presented in clear text for the user, otherwise it may be copied and disseminated.

Further, the solution depends on the decoder/displayer being itself is secured against copying. This may be achieved by embedding the decryption keys in a tamperproof way, protecting the keys from reading or modification or physical or logical circumvention. This would result in the displayer unit being secured for copying, essentially because the decryption key (and possible non-disclosed algorithms) cannot be read.

A CSS implementation using a tamperproof hardware ‘decoder and displayer’ would satisfy the requirements set out above. A CSS implementation using a software only ‘decoder and displayer’ hardly satisfies any of these requirements. The protection is at least much weaker than what can be achieved in electronic chips.”

CSS makes it therefore necessary for the purchaser of a DVD disk to have special equipment which can decrypt the encrypted DVD movie. The equipment may consist either of a DVD player in the form of a household appliance, hardware, which is linked to a television set for performing the movie, or a computer program, software, which is installed on a PC in such a way that the DVD disk may be read by the PC. In a PC the DVD disk is placed in the DVD drive, communicating by a data bus with the DVD-player in the form of a computer program.

A DVD disk with CSS encrypted material includes a disk key encrypted with a selection of approximately 400 so-called play keys. A DVD player must contain at least one of these play keys for the DVD movie to be performed in decrypted form. The producers of DVD players must therefore have access to at least one of the play keys to produce a DVD player which can perform encrypted DVD-movies.

CSS consists of several forms of protection in the form of codes or keys which are layered. The title key is used to encrypt the movie itself. Then the title key is encrypted with a disk key. The disk key is encrypted with a selection of the approximately 400 play keys. A DVD

player which has access to at least one play key can decrypt the disk key, using this the title key may be decrypted, and the content of the disk may be seen or heard in decrypted form.

All who want to produce such a DVD-player may request a license for this, and in such a way gain access to one or several play keys. The license is controlled by DVD CCA. The condition for obtaining a license is that the licensee observe confidentiality with respect to the play keys, and that they are protected in the DVD player in such a way that the purchaser of a DVD player cannot retrieve the play keys. Reference is made to the explanation of Hoy during the main hearing.

Not all producers of software accept such conditions, for instance a number of producers under the operating system Linux. The reason is that many of the programs made for Linux have an open source code, implying that anyone can see how the program is constructed. The objective is to enable anyone who wants to further develop computer programs for Linux. For this reason, there was no DVD player available for Linux in the autumn 1999. Reference is made to the explanation of Johansen himself, and that the explanation in this respect has not been disproved.

In addition to the encryption, CSS consists of an authentication which is to limit DVD-movies protected by CSS to being played only by players produced under license from DVD CCA. The authentication means that the DVD drive with the DVD disk and the player accept each other, and that the DVD player is given access to the content of the DVD disk.

The CSS also includes a zone control. The world is divided into different zones where for instance USA is zone 1 and Europe with parts of Asia is zone 2. A DVD disk contains information about which zone it is purchased in, and it should only be able to be played by DVD players purchased in the same zone.

The development of DeCSS.

Johansen has explained that in autumn 1999 he wanted to play DVD-movies under the operation system Linux.

Through several chat channels on the Internet, *Johansen* established contact with other persons who shared his interests. The conversation on the chat channels could either be “open” with all who had logged on, or “private” between two persons. One of the more important chat channel services for this case is IRC (Internet Relay Chat). *Johansen* was the autumn 1999 operator of the chat channel PCDVD. The nickname of *Johansen* for the chat channel was “MultiAGP”.

At page 326 in the factual extract⁵ is included a print-out of an IRC log showing a conversation of 11 September 1999 between *Johansen* and a person calling himself “mdx”. The print-out discloses that *Johansen* and “mdx” discuss how one would be able to discover the decryption algorithm to CSS by identifying a DVD player which did not protect, or has low protection, of the play keys. At page 328 in the factual extract is included a print-out of a conversation 22 September 1999 on IRC between *Johansen* and “mdx”. It discloses that a person going under the name “the nomad” has the program code for the decryption algorithm in CSS. The print-out further discloses that “mdx” communicated this program code to *Johansen*. This is also confirmed by the explanation of *Johansen* during the main hearing. *Johansen* has further explained that “the nomad” found the decryption algorithm in CSS by reverse engineering of a DVD player by the brand Xing. This is also disclosed by the conversation between *Johansen* and “the nomad” on IRC 24 September 1999, included in the factual extract page 393.

Johansen has further explained that program code for the authentication algorithm in CSS was published on the news group Livid on the Internet. Livid is a news group for persons

⁵ This is made available to the court from counsel for the prosecution.

interested in developing programs under the operating system Linux. *Johansen* could during the main hearing not remember how he gained access to the program code for the authentication algorithm. But it has not been proved that *Johansen* participated in developing this program code. The court therefore bases its decision on the fact that *Johansen* retrieved or received this after its development was finalised. *Johansen* has explained that he later has learned that it was a person named *Derek Fawcus* who had found the program code for the authentication algorithm in CSS.

The court finds it proven that *Johansen* combined the program code for the authentication algorithm and the program code for the decryption algorithm and developed a user interface. In this way, the computer program DeCSS was developed. The user interface was designed for the program to be run under the operation system Microsoft Windows.

The court finds it proven that DeCSS makes a decrypted copy of an encrypted movie, and stores this on the hard disk of the computer. References are made to the explanation of *Svein Yngvar Willassen*, special investigator at Økokrim, and the demonstration of the program made during the general hearing. This also corresponds to the explanation of *Johansen*.

At page 393 in the factual extract is included a print-out of an IRC log with a conversation of 24 September 1999 between *Johansen* and “the nomad”. The print-out discloses that *Johansen* has made a CSS decryption program using the program code of “the nomad”, and added a GUI (Graphical User Interface), a user interface making the program easier to use. It is also disclosed in the same page of the print-out that *Johansen* requested “the nomad” to test this program. *Johansen* requested also “the nomad” for permission to publish the program, a requested accepted by “the nomad”.

Johansen has explained that DeCSS was tested in the period ending by the program being made available on the Internet. *Johansen* has also explained that several versions of DeCSS were made. Willassen has explained that several versions of DeCSS were found during the search at the home of *Johansen*. The court therefore bases its argument on the fact that several versions of the program were made. *Johansen* is not certain which version was made available on the Internet. The court does not find this critical for the case.

Johansen has explained that on 6 October 1999 he either published a link, or made the program directly available at his home page on the Internet. The same day he sent a message to Livid, included in the factual extract page 20. In the message *Johansen* states that DeCSS is a CSS decrypter working for the movie “The Matrix”. A similar program, “DoDs speedripper” did not work for this. *Johansen* states further that the program works under the operating systems Win98 and Win2k. He then states where on the Internet the program can be retrieved.

At page 450 in the factual extract is included a print-out from an IRC-log with a conversation of 6 October 1999 between *Johansen* and “the nomad.” It is disclosed that *Johansen* by an error has “uploaded the source.” The court interprets this as a reference to DeCSS, which had been made available on the Internet, and refers to his communication to “the nomad” that he would attempt to make those who had downloaded the program to delete their copies. *Johansen* has explained that he deleted the source code from the Internet. The reason was that they did not want DVD CCA to withdraw the Xing key, disabling DeCSS. The court takes as proven that *Johansen* withdrew the source code from the Internet shortly after it has been made available.

The source code of DeCSS was made available on Livid 25 October 1999. The sender was anonymous. At page 501 in the factual extract is included a print-out of an IRC-log disclosing a conversation between “the nomad” and *Johansen* of 25 October 1999. The print-out discloses the irritation of *Johansen* caused by someone having made the source code of DeCSS available because the code included the play keys of the Xing player. DVD CCA

could therefore have reacted by withdrawing play keys. The court finds on this basis that it is proven that *Johansen* did not publish the source code of DeCSS at this time.

Johansen, however, has explained that he made the source code available on the Internet at a later time because it then already had been made available.

Johansen has explained that prior to the development of DeCSS there existed programs for the decryption of DVD-movies. One of these programs have been mentioned above, "Speedripper". The program was developed by a group known as "Drink or Die" (DoD). According to *Johansen* this program did not work for several movies, including "The Matrix".

The disclosure of play keys

At page 537 in the factual extract is included a e-mail of 7 October 1999 from a person called *Brian Demsky* to *Johansen*. The e-mail discloses that *Demsky* has downloaded DeCSS, and that he has made a program to identify the approximately 400 play keys. The objective was to prevent DeCSS from being disabled if DVD CCA should withdraw any of the play keys. This is confirmed by *Johansen* during the main hearing.

At page 538 of the factual extract is included the response from *Johansen* to *Demsky* the same day. *Johansen* wrote that this was good news, and that there was an interest in this.

In the program code of the decryption algorithm that *Johansen* received from "the nomad" was embedded at least one play key. At page 459 in the factual extract is included a print-out from an IRC log which discloses a conversation between *Johansen* and "the nomad". The log discloses that *Johansen* only at this time understood the function of the play keys. The log further discloses that *Johansen* communicated play keys he had received from *Demsky* to "the nomad." It is further disclosed that "the nomad" tested several of the play keys, and that *Johansen* should communicate the results of the tests to *Demsky*. *Johansen* has explained during the main hearing that he can not recollect that he himself took part in the testing, but that he communicated play keys and test results between *Demsky* and "the nomad". From the log, no certain conclusion can be inferred with respect to the participation of *Johansen* in the testing of the play keys. The court, however, does not find this critical for the case as it is not disputed that *Johansen* mediated the contact between *Demsky* and "the nomad".

At page 553 in the factual extract is included a print-out of an e-mail of 9 October 1999 from *Demsky* to *Johansen*. The e-mail discloses that *Demsky* has identified approximately 400 play keys, and that he has mailed them to *Johansen*.

After a while, the breaking of CSS became known by the media. At page 674 in the factual extract is included a print-out of an article on the Internet in November 1999 where *Johansen* frames himself as a spokesman for the group MoRE (Masters of Reverse Engineering), the group that broke CSS. *Johansen* has explained that his father was contacted by attorney-at-law *Erik Tøndel*, who on behalf of MPA asked *Johansen* to delete DeCSS from the Internet. *Johansen* complied with this request from *Tøndel*, and removed DeCSS from the Internet. *Johansen* has further explained that he once more made DeCSS available to the Internet the following week-end, and that it was available until 24 January 2000.

Amendment of the indictment during the main hearing

As the indictment was formulated at the beginning of the main hearing, *Johansen* was indicted to have gained unauthorised access to the data on the DVD disk. As the indictment was formulated, "data" could refer to both the movies themselves, but also other data stored on a DVD disk. During the main hearing the counsel for the prosecution made the indictment more precise by the sentence "*Jon Lech Johansen* accessed the undisclosed key storage in CSS". The counsel for the defence has claimed that this is a different matter than what originally was referred to in the indictment, and that the matter is precluded with reference to the penal code section 67 first paragraph. The court finds that this is not a different matter

than referred to in the original form of the indictment. The court has certain sympathy for the argument of the counsel for the defence that the counsel for the prosecution was somewhat less than precise with respect to what the indictment referred to, but finds regardless that the form of the indictment has to be accepted.

The issue of guilt

The penal code section 145 first and second paragraph reads:

“He who without authorisation breaks a letter or a closed and written document or in a similar way gains access to the content, or breech the locked keeps of another is to be punished by a fine or prison up till 6 months.

The same applies to he who by breaking a protection or in a similar way without authorisation accesses data or programs stored or communicated by electronic or other technical means.”

Therefore, to find *Johansen* guilty with respect to the penal code section 145 second paragraph, he himself must have, or he must have co-operated with someone who has broken a protection or in a similar way gained access to data or programs. Originally the penal code section 145 applied to he who “without authorisation broke a letter or a closed and written document or breeched access to the locked keeps of another or co-operated in this”.⁶ The provision was amended by a statute of 16 February 1979 no 3. A second sentence was then added to the first paragraph, which read:

“The same applies to he who without authorisation gains access to the content of a closed communication or note when this normally only is accessible using special equipment for connection, playing, listening, reading *etc.*”

NOU 1985:31 *Computer Crime*⁷ explains page 43 that the provision applied to access to data stored in computerised form. At pages 29 and 30, the Penal Code Commission discusses the need for amendments to section 145. From page 30 the court cites:

“The words of the provision (‘a closed communication or note’) are not immediately associated with information stored on a computer, and there are reasons to believe the provision is not well known among computer experts. The Penal Code Commission has therefore edited the provision (as section 145 second paragraph) without intending any substantive amendment.”

The proposal of the Penal Code Commission to section 145 second paragraph is the provision in its current form. As the Penal Code Commission did not intend to make any substantive amendments, legal sources associated with the former version will still be relevant.

In Ot prp no 35 (1986-87)⁸ at page 20 ff the Ministry of Justice⁹ discusses the requirements to be found guilty according to section 145 second paragraph. At page 20, the ministry

⁶ This citation is in old-fashioned language, no attempt has made to retain this quality in the translation, but this explains the rather odd choice of words both in the current and original form of the first paragraph.

⁷ NOU is a series of reports published by the government, in this instance the report is from a standing expert committee, the Penal Code Commission, proposing amendments to meet the challenges of computer crime, the original title in Norwegian is *Datakriminalitet*. This report is considered part of the legislative history of an act, though the proposed amendments will have to be proposed formally, of often in an amended form, by the government in a bill to the parliament. In Norwegian legal tradition, interpretation of statutes relies heavily upon the legislative history.

discusses the phrase “breaking a protection or in a similar way”. From page 20, the court cites:

“By including ‘in a similar way’, the interpretation of the requirement to break a protection becomes less definitive. The point is that section 145 only shall apply to cases where the act of gaining access to data should be characterised as qualified unjustified. To break a protection is such a qualifying element, but one may consider similar situations where the act of gaining access to data is sufficient serious that section 145 should be applied (...) Otherwise, the decision to apply the section has to be based on a judgment where also other elements associated with the act and the context of the act may be considered.”

The essential element in the phrase is therefore “without authorisation.” The Penal Code Committee writes on page 15 this about the concept ”without authorisation:”

“In principle it relies on the law and on contracts what data a person is authorised to access.” (NOU 1985:31 *Computer Crime*.)

At the same page, the Commission writes:

“The expression ‘without authorisation’ is associated with the different data elements and not to the data storage as such.”

The formulation indicates, as does formulations in the government bill, that the issue of unauthorised access must be associated with the issue of whether a person is authorised to gain access to the computerised data, not to how the person gains this access.

The court therefore interprets the provision not to apply to the person who in a different way than presumed by the producer, gains access to data to which he otherwise is authorised to access. This must hold also if access is gained by breaking a protection or a similar method.

Access to the movie

The court finds that a person purchasing a DVD movie, which is legally produced, is authorised to see the movie. It would be different if the DVD movie was produced illegally by copying in violation of the copyright act, so-called pirate copying. The owner of a pirate copy will therefore not have a lawful claim to see the movie.

As mentioned above, the court finds it proved that DeCSS makes an decrypted copy of an encrypted DVD movie, which is stored on the hard disk of the computer. The court there bases its argument on the fact that the use of DeCSS gives the user access to the movie in a decrypted form. That a copy is made is, according to the opinion of the court, not decisive as the making of a copy itself is not a violation of the penal code section 145.

The issue before the court is therefore whether Johansen has used DeCSS for DVD-movies produced illegally and which he therefore was unauthorised to access.

At page 299 in the factual extract there is included a print-out from a chat channel 9 October 1999 between *Johansen* and a person calling himself “Robshot”. It is disclosed from the print-out that *Johansen* has pirate copies of computer programs. There is further disclosed by page 474 of the factual extract, which is a print-out of an IRC log of 14 October 1999 between *Johansen* and “the nomad” that *Johansen* has an illegal copy of the program

⁸ Ot prp is an abbreviation for “Odelstingsproposisjon”, a bill from the government to the parliament, which for legislative purposes is divided into two chambers, the Odelsting and the Lagting. This is generally the source most useful for interpretation of statutes.

⁹ The bill is in this case issued by the Ministry of Justice, and forwarded through the cabinet.

Scenarist 2.0. *Johansen* has explained, however, that he has not had illegally copied DVD-movies. He has explained that he used DeCSS on the movies “The Matrix” and “The Fifth Element”, and that he purchased both movies legally in shops respectively in Oslo and Larvik. It has not been proven that *Johansen* has used DeCSS for illegally acquired movies. The court therefore concludes that he cannot be convicted with respect to the penal code section 145 second paragraph for his own use of DeCSS.

The next issue to be considered is whether *Johansen* can be convicted for co-operating in a violation of the penal code section 145 second paragraph by the unauthorised access to DVD-movies by others. Under penal code section 145 fourth paragraph, co-operation is also criminal.

From page 200 in *Erling Johansen Husabø's* book *The periphery of criminal liability – co-operation, attempt, preparation*¹⁰ (1999) the court cites:

“The statements [in the legislative history to the penal code] imply that even if the person who co-operates has done what is necessary, one should not punish the co-operator for more than an attempt as long as the principal has not completed the crime.”

There has been no proof of DeCSS having been used by anybody for illegally acquired DVD-movies. Reference is made to the explanation of special investigator *Willassen* during the main hearing that he did not know of concrete examples where DeCSS had been used for illegally acquired DVD-movies. *Johansen* therefore cannot be convicted of completed co-operation.

The court also has to decide if *Johansen* can be convicted for attempted co-operation. The issue is if *Johansen* can be convicted for co-operation by producing and publishing a tool which make it possible for others to gain unauthorised access to DVD-movies.

The current case has similarities with the trade in goods discussed by *Husabø*. From page 100 in his book the court cites:

“Nearly any type of goods can be used as a *means* to a criminal act. Also, certain types of goods have a certain probability of being used in such a way. But even so there is full consensus that criminal liability normally is excluded for both producer and seller (...) What motive the producer or seller might have had, is therefore generally not relevant ...

As long as the goods also serves legal purposes, the problem is not as much to justify lack of criminal liability as to justify this when a sale to another may trigger criminal liability for co-operation.”

The point of departure, therefore, is that trade in goods which have a legal purpose, cannot be punished as criminal co-operation. The same must hold for the distribution of products. The decision therefore relies on whether DeCSS has a legal area of application.

As stated above, the court does not hold that it would be a violation of the penal code section 145 second paragraph to use DeCSS for seeing DVD-movies which are legally acquired. Neither it is not a violation of the penal code 145 second section to produce copies of legally acquired DVD-movies for private use, cf. the copyright act section 12. DeCSS can therefore be used both to make a copy of a DVD movie and view a DVD movie if one does not have licensed equipment. How useful this is for the society may be subject to different views, but it would appear that it is lawful. The court therefore holds that DeCSS can be used both lawfully and unlawfully.

¹⁰ Norwegian title: *Straffansvarets periferi – Medvirkning, forsøk, førebuing.*

The Supreme Court has convicted someone for criminal co-operation for the sale of goods that otherwise were legal, cf. Rt 1996 page 965.¹¹ The Supreme Court decided the case on the fact that the organisation of the trade clearly showed that the purpose of the perpetrator was to sell goods that exclusively was to be used for the illegal production of alcohol. The purpose of the perpetrator therefore is an important element deciding whether someone can be convicted for co-operation. But according to *Husabø*, the decision must be based on an objective view of the apparent circumstances in the case, cf. *Husabø* page 117.

In the current case, the court finds it difficult to make any certain conclusions with respect to the purpose of the development by Johansen of DeCSS and the publishing of the program on the Internet. *Johansen* has explained that the purpose was to contribute towards the development of a DVD player for the operating system Linux. At page 885 in the factual extract is included an e-mail of 12 September 1999 from “the nomad” to *Derek Fawcus*. It is disclosed by the e-mail that “the nomad” mailed the program code for the decryption algorithm in CSS to *Fawcus*. In the e-mail, “the nomad” also writes that he hopes this will contribute towards the development of a DVD-player for Linux.

Johansen has expressed himself in a negative way with respect to the operating system Linux and the development environment for this system. At page 45 in the factual extract is included an e-mail of 6 October 1999 in Livid from a person called *Michael Holtz*. *Holtz* writes that *Johansen* said that he hates Linux, and would be happy if the system never had been invented as FreeBSD is much better. At page 47 in the factual extract is included the response from *Johansen*, where he wrote that he never had said that he hates Linux, but that it would not have mattered if Linux never had been invented because FreeBSD is so much better. At page 51 is included an e-mail of 8 October 1999 to Livid where *Johansen* deplore his attitude in earlier e-mails, and writes that Linux is a very good operating system, but that FreeBSD is even better. At page 458 and 459 in the factual extracts is included a print-out from an IRC-log with a conversation 8 October 1999 between *Johansen* and “the nomad” where *Johansen* says he has mailed his excuse to Livid, but that this only was to satisfy another person, whom the court presumes to be *Derek Fawcus*. *Johansen* further writes:

“God damned linux fanatics, I wish someone would shoot them ;)”

From the context, and on the basis of the explanation of *Johansen* during the main hearing, the court presumes that the basis of this statement was a conflict between *Michael Holtz* and *Johansen* with respect to whether the source code of DeCSS should be published, and the circumstances around the communication of the source code to *Fawcus*. The court therefore finds that the statements of *Johansen* with respect to Linux cannot be taken literally, and that they do not clearly represent the attitude of *Johansen* towards Linux in general. The court therefore finds that this correspondence is insufficient proof for the purpose of *Johansen* in developing DeCSS.

The little interest *Johansen* took in Linux at the time when DeCSS was made, however, does weigh against the argument that the purpose was to develop a DVD player for this operating system. It is evident from what is stated above that, in the opinion of *Johansen*, FreeBSD was a better operating system than Linux. It is also disclosed by a conversation between *Johansen* and “the nomad” on IRC included at page 506 in the factual extract that *Johansen* as late as 26 October 1999 had not had Linux installed on his computers.

It also does weigh against the argument that the purpose of *Johansen* was to develop a DVD player for Linux that he made DeCSS as a Windows program. However, *Johansen* has

¹¹ The reference is to the reporter for the Supreme Court, Norsk Retstidende, generally abbreviated Rt. The reference is to the volume and the first page of the published report.

explained that he lacked knowledge of Linux, and that support for UDF (the file system on a DVD disk) was missing for this operating system.

Johansen made DeCSS available on the Internet, and he was concerned that the program should be simple to use “by the average joe”, cf.428 in the factual extract, which is a print-out from an IRC log with a conversation between *Johansen* and “the nomad” 5 October 1999. *Johansen* has explained that it was necessary to publish DeCSS on the Internet to test the program and correct errors, and then be able to develop the program further. The court cannot see, however, that any of the improvements made after 6 October 1999 contributed towards the development of a DVD player for Linux.

At page 29 in the factual extract is included a print-out from a chat channel for two conversation 12 September 1999 between *Johansen* and “Robshot”. The print-out discloses that a person calling himself “Wag” maintains that the chat channel of which *Johansen* is operator, PCDVD, only is concerned with pirate copying. In the conversation is cited a conversation between *Johansen* and “Wag”, where *Johansen* wrote the following to “Wag”:

“and I’ve got only one thing to say to you, keep out of # PCDVD, we are criminals in there, you don’t want to mingle with us.”

At page 366 in the factual extract is included a print-out from a log of a chat channel with a conversation of 25 September 1999 between *Johansen* and a person calling himself “Terryben”. The print-out discloses that *Johansen* wrote the following to “Terryben”:

“so, hehe, we’ll be copying dvds in notime when dvd burners drop in \$”

The court finds it difficult to place too much weight on the print-outs from the chat channels with respect to the purpose of *Johansen* for the development of DeCSS. Reference is especially made to pages 395, 396, 435, 464, 468, and 512 in the factual extract which are print-outs from conversations between *Johansen* and “the nomad” where there is many references to the development by DoD of a decryption program.

On this basis, the court finds that it is not proven above reasonable doubt that the purpose of *Johansen* with the development and publishing of the program was to contribute to the illegal copying and distribution of DVD-movies.

The court has after this concluded that *Johansen* cannot be convicted for co-operation to the violation of the penal code section 145 second paragraph with respect to accessing the movies. This also holds even though *Johansen* knew that the program could be misused. This holds for anyone who distributes goods which may be put to lawful or unlawful use.

Access to the play keys

The next issue is whether *Johansen* can be convicted for violation of the penal code section 145 second paragraph with respect to the play keys in CSS. For *Johansen* to be convicted for the violation of the penal code section 145 second paragraph with respect to the play keys, there also in this respect has to be the breaking of a protection or a similar action giving unauthorised access to these.

In Ot prp 35 is discussed the condition “breaking a protection or in a similar way”. From page 20 the court cites:

“The Ministry does initially agree with the Penal Code Committee that the provision should be written in such a way that it only can be applied when the offended has done something himself to protect the information against unlawful access.”

It is therefore required that the information in fact is protected against access, and that the purpose is to protect against unauthorised access. The court presumes that the strength of the protection is not relevant. It must be sufficient that the offender has done *something* to protect the information. On the other hand, the court presumes that circumstances which make access difficult shall not count as protection with respect to the penal code section 145 second paragraph if the purpose has not been to protect against unauthorised access.

Johansen has explained, and the court bases its argument on the fact that “the nomad” wrote the program code for the decryption algorithm in CSS after he had reverse engineered a Xing player. The issue is then whether the reverse engineering implies a violation of the penal code section 145 second paragraph. *Johansen* has explained that he by reverse engineering indicates the analysis of a computer program to determine its functions. According to *Johansen*, “the nomad” had understood the decryption algorithm in CSS and written a program for this in a high level language. This program “the nomad” mailed to *Johansen*.

Reverse engineering is not mentioned in the legislative history of the penal code section 145. Considering the application of the penal code section 145 second paragraph one will have to take into account the principle of legality,¹² which is interpreted rather strictly in the area of criminal law, cf. the Constitution sect 96. The Supreme Court has in two decisions interpreted the penal code section 145 second paragraph very strictly with respect to the natural understanding of the provision, cf. Rt 1994 page 1610 and Rt 1995 page 35.¹³ The decisions relate to the word “data”, but can be interpreted more generally as a directive for a very narrow interpretation of the penal code section 145 second paragraph.

Bjørn Bjerke gives in his book “*Reverse engineering*” of computer programs (1994)¹⁴ at page 23 the following definition of reverse engineering:

“Reverse engineering is thereby a process through which one derives an understanding of data and processes in an existing computer system. The objective is to extract contents, structure, and data flows from existing computer programs and represent this information in a form appropriate for further analysis and documentation.”

At page 24 *Bjerke* discusses the different strategies for reverse engineering. First, one may read about the program in available manuals and literature. Second, one may observe the program under execution. The court finds it obvious that the two first methods do not represent a violation of the penal code section 145 second paragraph. *Bjerke* describes page 5 ff the third approach, called the dissection strategy:

“*The dissection strategy* presume that we can read and understand the program for extracting the information on the individual machine instructions, their function in the form of a description on a higher level of abstraction, and the place of these functions in the algorithm which describes what the program achieves. The computer program in its distributed form is in binary code, a long line of ones and zeroes, containing a lot of ‘fillers’ in addition to the original program ...

¹² The principle requires that any law determining obligations for individuals have authority in formal enactments[?].

¹³ Both decisions relate to conditional access to scrambled television, where an unauthorized smart card was used to give access to the broadcast. The decisions are also attracted critical comments in the literature, but are very clear with respect to what is mentioned in the text above.

¹⁴ *Bjørn Bjerke* “*Reverse engineering*” av datamaskinprogrammer, CompLex 9/94, published for the Norwegian Research Center for Computers and Law by Tano, Oslo.

Even using alphanumerical symbols, the resulting code will not convey much meaning unless one is able to read the machine instructions and data. Said in other words, one will have to disassemble the program.”

Bjerke goes on to describe that disassembling means that the object code is transformed to assembly code. Disassembling can be performed by a disassembling program, but in addition one will have to conduct testing. The assembly code, too, is difficult to understand for a human, and decompilation will therefore be necessary. Decompiling is transformation of the assembly code to a high level computer language.

On the basis of the description by *Bjerke* on reverse engineering, and the explanation given by *Johansen* on how “the nomad” wrote the program code for the decryption algorithm in CSS, the court finds it difficult to qualify this as breaking a protection or a similar act. The court does not find it proven that the objective of distributing a computer program in object code is that the producer of the program has wanted to protect the source code. The objective may as easily be that the program in object code may readily be executed by the computer. Therefore, the court concludes that the reverse engineering by “the nomad” does not represent a violation of the penal code section 145 second paragraph.

The court finds it proved that the program code communicated to *Johansen* from “the nomad” at least contained one of the play keys of CSS. The issue before the court is therefore whether this or those were protected with respect to the penal code section 145 second paragraph.

John Hoy, the president of DVD CCA, has explained that the non-disclosure of the play keys was a condition for obtaining a license to produce a DVD player for viewing encrypted movies. This is not, however, sufficient to prove that all producers actually complied with respect to this condition. *Johansen* has explained that the Xing player did not have any protection of the play keys. This corresponds to what “the nomad” wrote to *Johansen* in the conversation on IRC 24 September 1999 included at page 394 in the factual extract. There has been no other evidence relating to the protection of keys in the Xing player. The court therefore concludes that there is no violation of protection or similar arrangements in relation to the play keys in the Xing player.

With respect to the other play keys, it is disclosed by page 537 in the factual extract that *Brian Demsky* 7 October 1999 contacted *Johansen* and told that he was in the process of identifying all play keys in CSS on the basis of the program code for the decryption algorithm in CSS which *Johansen* had made available on the Internet the day before. *Demsky* wrote also, “I’m currently at a key rate of 2.5 million keys/sec/450 mhz”. This indicates that he had developed a program which made it possible for the computer to guess possible play keys. The basis of the program is the decryption algorithm in DeCSS where the Xing key was located. The court finds that though this procedure itself represents the breaking of a protection, or at least is included in the phrase “in a similar way”, this breaking of a protection does not give access to data. The penal code section 145 second paragraph does not apply to the breaking of the protection itself if the perpetrator is not given unauthorised access to data. As stated above, the court has concluded that applying DeCSS to movies which have not been illegally produced or acquired, does not represent a violation of the penal code section 145 second paragraph.

With respect to the issue of co-operation, reference is made to the discussion above relating to the movies. Also with respect to the possible use by others of the play keys to gain unauthorised access to information on DVD disks, the court finds that *Johansen* cannot be convicted for an attempt of co-operation. The court therefore finds that *Johansen* cannot be convicted for co-operating in the violation of the penal code section 145 second paragraph with respect to the play keys.

Johansen will after this have to be acquitted.

Seizure

The counsel for the prosecution has in the indictment claimed seizure of one PC cabinet Pentium III 500 MHz and 8 mixed software not licensed, referring to the penal code section 35 second paragraph. The court does not find it proven that the objects have been used for, or have been intended to the use for a criminal act. The claim of seizure is refused.

Costs

The counsel for the prosecution has claimed that *Johansen* shall pay the costs of the proceedings. *Johansen* is acquitted and can therefore not be instructed to pay the costs of the proceedings, cf. the criminal procedure act section 436 first paragraph.

The decision is unanimous.

Sentence:

I

John Lech Johansen, born 18 November 1983, is acquitted.

II

The claim for seizure is refused.

III

Costs of the proceedings are not to be paid.

Irene Sogn
Assistant judge

Terje Knudsen
Senior engineer

Stein Marthinsen
College lecturer