

# Jon Bing

Professor, dr juris

Bøgata 7, NO-0655 OSLO – Norway

Phone: +47-22-675400, fax: +47-22-677478, mobile: +47-90-967659

E-mail: jon.bing@bing.no; jon.bing@jus.uio.no



## The Norwegian DVD case – Decision by Borgarting Appellate Court<sup>1</sup>

- Instance: Borgarting Appellate Court
- Date: 22 December 2003
- Published: LB-2003-00731<sup>2</sup>
- Key words: Computer crime. Assessment of evidence. Copyright act sects 4, 12 and 39i, criminal code sect 145 second paragraph.
- Abstract:<sup>3</sup> A young person had in 1999 with others co-operated to the development of a program that circumvented Content Scrambling System for DVDs, and posted this on the Net. He had programmed a user interface which made the program available also for persons without any special knowledge of information technology. The appellate court found, as the first instance court, at the development of the program was not illegal. The action was not found to be an infringement of the provisions of the copyright act. Therefore, access could not be qualified as ‘unauthorised’ according to the criminal code sect 145, second paragraph. The appeal of Økokrim<sup>4</sup> was therefore rejected.
- Citations:<sup>5</sup> [LOV-1902-05-22-10-§145](#) (Strfl), [LOV-1961-05-12-2-§12](#) (Åvl), [LOV-1961-05-12-2-§39i](#) (Åvl), [LOV-1961-05-12-2-§4](#) (Åvl)
- History:<sup>6</sup> Oslo first instance court TOOSLO-2002-00507 – Borgarting appellate court LB-2003-00731 M/02.
- Parties: The public prosecution (first public prosecutor Inger Marie Sunde) *versus* [A] (defendant attorney Halvor Manshaus).
- Author: Appellate court judge Wenche Skjæggestad, president.<sup>7</sup> Temporary appellate court judge Endre Stavang and extraordinary appellate court judge Hjamlar Austbø. Lay judges: President of the institution Bente Brunvatne. Sheet metal worker Morten Midtun. Senior consultant Dag Asheim. College professor Martion Gilje Jaatun.

---

<sup>1</sup> The decision is translated from the original Norwegian proceedings 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 translation may in detail be inaccurate. The translation may freely be reproduced and made available by third parties, and no copyright is vested in the original decision, cf the Norwegian copyright act sect 9. All notes to this decision are the responsibility of the translator. The original Norwegian decision is available from the information system of Lovdata (<http://websir.lovdata.no/lex/frame-eu.html>).

<sup>2</sup> Index number for the Lovdata foundation legal information system.

<sup>3</sup> The abstract is developed for Lovdata, the national legal information service of Norway, the abstract is authored by the judge.

<sup>4</sup> Special central division of the public prosecutor for economic and similar types of crime.

<sup>5</sup> These links will work, and give access to the original Norwegian acts.

<sup>6</sup> These citations are to the Lovdata foundation information system.

<sup>7</sup> The decision will have been drafted by the presiding judge, any dissident judges will append their own minority report.

[A]<sup>8</sup> is born in 1983 and lives in –street --, Oslo. He is a student, not married and without family responsibilities. By indictment of Økokrim, amended twice, the latter amendment of 13 December 2002, he was prosecuted by Oslo first instance court for breaking:

**The criminal code section 145 second of third and fourth paragraph**

by having broken a protection or in a similar way unjustified accessed data stored or communicated by electronic or other technical means and by having caused harm by exploiting or using such unjustified information, or having contributed to this.

**The basis is the following actions, or contributions to these**

In the period September 1999 – 24 January 2000 by Internet from his home in X, [A] participated in breaking the technical protection system Content Scrambling System ('CSS'), licensed by DVD Copy Control Association Inc, to protect DVD movies produced by Motion Pictures Association to prevent copying. A DVD movie is a movie stored in electronic form on a DVD disk. On the basis of knowledge of a secret algorithm and play keys incorporated in CSS, [A] developed the Windows program DeCSS, Using DeCSS results in an unprotected copy of the movie. [A] used DeCSS for his own DVD movies, and he made DeCSS several times available in different versions over the Internet in the period indicated above. By the actions described [A] gained unjustified access to the key storage of CSS. [A] also broke the copy protection of the DVD movies and made access possible for himself and others to the data of the DVD disks in a form not protected. Access was unjustified because the DVD movies were sold on the condition that the users only should used authorised playing equipment and respect the copy protection. Accessing the movies in a form not protected has caused harm as the rightholders no longer have protection against unjustified distribution of the movies.

General considerations requires<sup>9</sup> prosecution.

Oslo first instance court decided the case 7 January 2003 with the following rendition:

- I. [A], born \*\* 1983 is acquitted.
- II. The claim for seizure is not accepted.
- III. Litigation costs are not awarded.

For the details of the actions and the personal data of the defendant, reference is made to the decision by Oslo first instance court and the remarks of the appellate court below.

The prosecution, Økokrim, had appealed the case in time to Borgarting appellate court. The appeal which refers to the application of the law under the issue of guilt, procedural matters and some aspects of the assessment of evidence, was referred to appellate procedure at the appellate court by a decision of the appellate court of 17 February 2003.

The appellate proceedings were heard in the period 2 to 11 December 2003. Two of the four lay judges, senior consultant Dag Asheim and college professor Martin Gilje Jaatun, are experts in information technology and named from outside the selections, cf the act on court proceedings sect 88. The defendant and seven witnesses were heard. Four of the witnesses

---

<sup>8</sup> The case report is anonymous according to the principles of data protection observed by Lovdata.

<sup>9</sup> Appellate courts may use lay judges in addition to the legal judges, there are pre-nominated selections from which the lay judges are drawn in normal circumstances. If the court finds that certain expertise is needed in the panel of judges, appropriate lay judges may be named.

were heard as experts without being named by the court. The documentation is contained in the records of the court.<sup>10</sup>

**The claim of the prosecution:**

1. [A], born \*\* 83, are sentenced according to the indictment to a punishment of jail in 90 – ninety – day, which are made conditional with a trial period of 2 – two – years, cf the criminal code sect 52 *etc.*
2. [A], born \*\* 83, are sentenced to endure seizure of
  - a. One PC cabinet Pentium III 500 Mhz (seizure A-2), cfr the criminal code sect 35 second paragraph.
  - b. 8 CD-ROMs containing unspecified computer programs which are not licensed (seizure A-4-6), cf the criminal code sect 35 second paragraph.
3. [A], born \*\* 83, are sentenced to carry the expenditure of the case with 20,000 – twenty thousand – NOK.

**The claim of the defendant:**

The appeal is dismissed.

**The remarks of the appellate court:**

The investigations of [A] started in January 2000 after Motion Pictures Association and DVD Copy Control Association Inc. (hereafter DVD CCA) had brought charges to Økokrim. The DVD CCA foundation was formally created at the end of 1999. The objective was to organise a control scheme which, among other things, should stop piracy copying of DVD movies. It is notorious that piracy copying is a major problem for the movie industry. The movie industry launches most movies to different dates in the different markets. Economically it is important for the movie companies to control in which order the markets have access to the individual movie. According to the witness Martha King, Warner Home Video, it costs the members of the Motion Picture Association an average of 88 million<sup>11</sup> USD to produce and market a feature movie. Only 20 per cent of the movies make a profit. The markets for video and DVD has over time become those generating the largest incomes. For Warner Brothers the income from these markets amount to 60 per cent. Of this share, DVD amounts to 80 per cent.

Zone coding is an important control measure for the producers. It has been difficult to launch the movies in all markets simultaneously, for instance it has been difficult to produce a sufficient number of ‘master copies’. For many countries, the movies must be dubbed or subtitled. The producers also will often want to consider the sales in USA as this traditionally is an indication of the popularity in other continents. Also, censorship in some countries may make problems for simultaneous publication.

Among other things, the fact that the movies are launched at different dates has created a market for pirate copies. This form of copying has for a long time been a large and expensive problem for the movie industry. There have been developed rigorous guidelines for how the companies themselves handle their copies. The most serious alternative is an unauthorised copying of a movie that still has not been launched in all markets. Many illegal methods have been used, and one has for instance discovered copying using hand-held cameras during the performance. This method, however, results in a inferior copy compared to the original.

The DVD medium is digital, and makes it possible to produce perfect copiers if one has access to the data on the DVD. For obvious reasons the movie industry was initially rather reserved with respect to using DVD as a medium before it was possible to protect the data

---

<sup>10</sup> The records of the court is generally made by the presiding judge, and contain a summary of the proceedings.

<sup>11</sup> That is 88,000,000.

against copying. This is the background for the development of CSS – Content Scrambling System.

On the basis of a contractual arrangement between the largest movie companies in the USA and DVD CCA, there was developed a licensing scheme. DVD movies should only be performed on players with Content Scrambling System produced on the basis of a license issued by DVD CCA. The licensing regime was open in the sense that anyone might acquire a license to produce a player against an annual fee, and agreeing to follow a set of rules. The licensee was assigned one or two play keys and agreed to protect this or those. The reason the court is not certain whether there are one or two play keys assigned, it that DVD CCA has not been willing to make the program available to the experts of Økokrim, as the play keys have been qualified as trade secrets. If a DVD player or a player program for a PC with a DVD drive are not configured in such a way that the key or keys are sufficiently well protected against copying, the licensee may according to the licensing rules be imposed to pay a large sum for damages to DVD CCA. In addition to encryption, the system consists of a mechanism for authentication which is designed to deny access for an unauthorised player to the key material on the DVD. The authentication implies that components must recognise each other before the movie is performed.

It is notorious that the encryption mechanism for CSS is weak. At the time the movie industry and the consumer electronic industry agreed to develop a system for secure distribution of content on DVD, US export law prohibited use of more than 40 bits encryption. There is no large effort involved in decryption of such encryption. The appellate court bases its consideration on a relative secure encryption at least using 64 bits. The banks secure data on the net with 128 bits, and must be considered very secure. When the witness Stevenson at the end of 1999 analysed the CSS algorithm with the objective to identify the film keys, it was demonstrated that it in reality only represented an effective protection of 16 bits. The encryption must on this basis be considered as very weak. Based on this analysis, Stevenson also made a program that was able to decrypt CSS in less than a second, and which allowed the performance of a DVD on non-authorised players without the necessity of using play keys.

As discussed above, pirate copying is a very large problem for both the movie and music industry. In Southeast Asia there are located facilities that produce legal DVDs during the day, and where the same facilities are used to illegal production during the night. With special equipment it is possible to copy the DVD directly preserving the encryption on the pirate copy. Both methods result in copies of the same high quality as the original. In International Intellectual Property Alliance 2001 Special 301 Report on Taiwan, there was reported an increasing number of sites involved in unauthorised production of digital media. The production capacity was the astronomical number of 1,8<sup>12</sup> billion disks annually.

The copying of movies on the Internet was not very practical in 1999. The speed for transferring data was not sufficient; it would require approximately 12 days to transfer a whole feature film without compressing on an ISDN-connection. Broadband was not generally available. A feature movie required up to 8 gigabytes storage capacity, which was more than offered by the PCs at that time. Copying was not very practical. A DVD burner cost in 1999 approximately 20,000 NOK,<sup>13</sup> and the DVDs used for copying had not sufficient capacity fore a whole movie, and was also difficult to purchase. Copying of CDs was simpler and less costly, but a movie required at least 3-4 CDs for storage, and the quality would be inferior to the original. Neither price nor quality made copying a serious menace. The appellate court bases its argument on the view that pirate copying has not been a primary

---

<sup>12</sup> That is 1,800,000,000.

<sup>13</sup> Approximately 2,500 USD.

objective in developing a player outside the DVD CCA system. This also is evident from the chat logs where among others [A] makes very negative statements on piracy.

The documented chat logs demonstrate that there were several groups and individuals knowledgeable in information technology that independently was engaged in developing a player outside the DVD CCA licensing scheme. According to the documented material, the first who successfully circumvented the coding was a Russian known as 'Landy'. At the end of April 1999 he succeeded according to the documents to tap decrypted movie data from a Power DVD player during the performance of the movie.

The reasons for many wanting to develop an independent DVD player were several. The appellate court recognises that decryption represented a challenge as such, but there were also other reasons. Many consumers disliked the system for zoning. This ensured that the movie companies could price movies differently in different markets. DVD movies are approximately 50 per cent less expensive in USA compared to Europe. In addition several retailers in Norway purchases movies targeted for other markets. All DVD covers indicate the appropriate zones, but the indication may be difficult to read for the general consumer. The consequence may be that Norwegian users risks purchasing a DVD movie from a Norwegian retailer which cannot be performed on the equipment they have available. There have been documented examples movies purchased at Akers Mic<sup>14</sup> in Oslo and a retailer in Arendal.<sup>15</sup> The same problem was experienced by persons purchasing DVD movies abroad for performing in Norway. This problem has over time become sufficiently pronounced that it today is possible to purchase authorised players with programs, in violation with the licensing terms, eliminates the zoning.

The appellate court recognises that not all software producers have been able to accept the licensing terms stipulated by DVD CCA. Producers of programs under the operating system Linux base their operations on the principle of open source code, allowing others to inspect the structure of the program. The objective is to encourage others to further develop the programs. In the autumn 1999 there were no DVD player available under this operating system, and a licence from DVD CCA could not be obtained due to the philosophy of open source code.

[A] was one of several waiting for the development of a player under the operating system Linux. Through Relay Chat (hereafter called IRC) he was able to contact persons with the same attitude. 11 September 1999 ha had a chat with 'mdx' on how to disclose the play keys of a software player with insufficient protection. From a chat between the same two persons 22 September, 'mdx' states that 'the nomad' has disclosed the code for the decryption algorithm in CSS, and that 'mdx' now would make this available to [A]. 'The nomad' was supposed to have disclosed the decryption algorithm though reverse engineering of a Xing DVD player where the play keys more or less were available without protection. In this way he gained information which made it possible for him to make to program CSS\_scramble.cpp. The chat logs dated 4 November 1999 and 25 November 1999 document that 'the nomad' made the reverse engineering on a Xing player he describes as illegal. As the case is presented to the appellate court, however, this was not known to [A] until 4 November.

With respect to the authentication code, the appellate court bases its argument on 'the nomad' getting access to this from the mail list LiVid (Linux Video), and that this was developed by Derek Fawcus. Form a posting dated 6 October 1999 is documented that Derek Fawcus had read the source code of DeCSS and compared this to his authentication package. It is further documented that, 'The author has copies this nearly word by word – he has only

---

<sup>14</sup> A well known retailer.

<sup>15</sup> A town at the south coast of Norway.

removed my copyright notice from the top text and a paragraph with comments, and give the functions new names'. The name was CSS\_auth.cpp.

After this one must recognise that the program later developed by [A], the user interface (Graphical User Interface) consisted of the decryption algorithm of 'the nomad' and the authentication package of Derek Fawcus. Developing the user interface made the program available also to users without any special knowledge on programming. The program was first published on the Internet 6 October 1999 after [A] had tested the program on the movie 'The Matrix'. For this he downloaded approximately 2.5 per cent – 200 megabytes – of the movie to the hard disk of his PC. This download is the only movie data [A] has stored on his PC.

The program DeCSS was over time improved and made available in different versions. The last version was, according to the information made available to the court, posted 9 November 1999. The program works under the operating system Microsoft Windows 98 and Windows 2000.

[A] has claimed that his objective in developing the program was to contribute towards a Linux player, on which the appellate bases its argument, and finds that the reason for the program made available operating under Microsoft Windows was that at this time there was no support for the file format UDF for Linux. [A] did not have sufficient knowledge of Linux to contribute to this end. The witness Stevenson has stated that the work of [A] made it easier for others to test their components, approaching the development of a Linux player. By a mistake of [A] the source code of DeCSS was made available on the Internet 6 October 1999. It was withdrawn the same day. The source code he wanted initially to keep secret because he was afraid the Xing keys would be withdrawn. In this case, DeCSS would cease to work. But the source code was posted anonymously on LiVid 25 October. It is documented by logs from this date that [A] chatting with 'the nomad' was irritated by the code having been 'released', but that they at this time had access to several keys, therefore this was of little practical consequence. Brian Demsky, who downloaded the code 6 October, had in the meantime developed a program which identified play keys. [A] was unaware of this technology, but he made play keys available to 'the nomad' who tested them. It is also documented that Frank Stevenson downloaded the source code 25 October. He developed a program that fully eliminated the need to know play keys.

[A] is charged with the violation of the criminal code section 145 second and fourth paragraph. The provision applies to a person illegally breaking a security scheme or in a similar ways accesses data or programs stored or communicated by electronic or other technical means. The provision is in the criminal code title 13 regarding crimes against the general peace and order.

The first issue is the interpretation of 'data'. The appellate court interprets the term in this case to include both the movie and the program of the Content Scrambling System. Understood in this way, it is beyond doubt that the case related to 'data' in the meaning of the law.

The next issue is the interpretation of 'illegally'.<sup>16</sup> [A] had purchased all his DVD movies regularly, and had the right to perform them. To be performed, the movies had to be decrypted. However, the assumption of the producer was that the movie in encrypted form should be intact after its performance, while the program DeCSS permits the storage of the movie in decrypted form on the hard disk. A stored movie may be reproduced, for instance by burning DVD or CD disks, and this was exactly what the encryption was meant to exclude. The appellate court has above based its argument of [A] not himself having stored a movie for later performance on his own hard disk, but must nevertheless decide whether gaining the

---

<sup>16</sup> In the translation, some of the flavour of the original Norwegian legal term is lost. A better term might be 'unlawful' or 'without any legal right'. It refers to a legal doctrine of some substance.

possibility for this in addition to the possibility for performance, is illegal. In the legislative history<sup>17</sup> is stated:

'By adding "in similarly ways" the interpretation of the condition to break a security scheme becomes less decisive. The point is that sect 145 shall apply in situations where gaining access to data must be characterised as illegal.'

The wording of the provision, compared to the fact that any use of DeCSS implies the reproduction of an unprotected version of the encrypted movie data stored on the hard disk of the user, makes it necessary to identify a basis making the use of DeCSS legal. One such basis is the copyright code sect 12 which authorises reproduction.<sup>18</sup> The wording indicates that this right is not qualified, but the legislative history indicates that the provision is to be interpreted narrowly.<sup>19</sup> To illustrate the appropriate assessment, it is stated:

'How large part of a work and the number of copies to be reproduced, will rely on the conditions of the case in question – for instance the category of protected work, the volume of the work, how large part of the work is reproduced in the copy, the character of the copies being reproduced and whether the copies reproduce the work in the same form as the basis for the reproduction, and what use will be made of the copies. For instance, it will in general not be permitted for personal use to reproduce as such as one complete copy of a book, or a whole issue of a journal available in the market.'

It is the opinion of the appellate court that there is a qualified difference between copying a feature movie and reproducing a whole issue of a journal or a whole book. The feature movie is stored on a medium prone to be harmed like scratches, nicks and cracks, while a book or a journal may be read over and over again without reducing the quality. The appellate court bases its opinion on a DVD being vulnerable to injuries to such an extent that the purchaser must be permitted to make a copy, for instance of a movie in which he takes a special interest in preserving. One cannot see that the use of DeCSS represent any great danger for illegal reproduction of DVDs in competition with the movie producers. The legal history and the Berne Convention art 9 stipulates a weighing of interests, but in this case it is the interpretation of the copyright act sect 12 as part of a assessment of criminal law which is the issue, and in such a legal context the unconditional form of the wording of the provisions must, according to the view of the appellate court, be given considerable weight.

The next issue is whether use of DeCSS nevertheless is illegal because the movie is sold with a prohibition against copying. The prohibition is printed on the cover, but one must base the argument on there not being a standardised text which can be found on all covers. The text is often in English, but may be in another language, for instance French. The text is not readily available, and it is printed with very small type.

A prohibition against copying would limit the right of the consumer compared to the copyright act sect 12, which permits reproduction of copies of published works for private use

---

<sup>17</sup> Reference is made to the government bill to the Parliament, Ot prp no 35 (1986-1987) *Om endringer i straffeloven (On amendments in the criminal code)* page 20 at the bottom.

<sup>18</sup> This is a clause authorising reproduction for private use, where 'private' is interpreted very narrowly (family, close friends).

<sup>19</sup> Reference is made to the government bill to the Parliament, Ot prp no 15 (1994-95) *Om lov om endringer i åndsverkloven med mer (On an act amending the act of copyright protection etc)*, page 38, second column at the bottom.

when this is not commercial. The appellate court finds that unilateral conditions with respect to a use which is permitted according to the copyright act cannot be held valid.<sup>20</sup>

‘The commission has the opinion that current law generally does not permit unilateral conditions limiting use permitted by the copyright act. This opinion is underpinned by policy considerations. Such conditions may be compared to private lawmaking which easily may distort the weighing of interests on which the act is based. This is especially relevant with respect to conditions integrated in copies of protected works which are produced as mass market goods. For a private condition to be valid, they must generally be accepted as contractual terms.’

In addition, the appellate court can not see that it is evident from anywhere on the DVD cover that [A] was limited to use authorised players. If it should be, as the prosecution claims, that this condition is evident from the use of the label ‘DVD’ on the cover, the court cannot see that this condition has been accepted as a contractual term by the consumer.

The issue is then whether the decryption program as such was acquired illegally. If this can be demonstrated, one will have to decide whether that this had the consequence that the data were accessed illegally.

The prosecution has first argued that the reverse engineering or the decompilation of ‘the nomad’ is not sufficiently comprehensive to be qualified as reverse engineering. He dissected the program, what is known as decompilation. The appellate court does not recognise this as an argument in the case. [The legislative history]<sup>21</sup> has the following remarks:

‘Computer programs from different vendors often follow different standards. A program in object code (machine code) will not disclose the ideas or principles for someone acquiring the code, and one is therefore dependent on reverse engineering of the object version to a source version to comprehend the underlying logic of the program.

‘Another method for reverse engineering is “decompilation”, as the process is termed in the directive. Decompilation imply that the machine readable code of the computer program is translated back to written source code, or something corresponding to the original source code. From this it is possible to make the analysis of the interface and the underlying principles.’

As the appellate court understands this, ‘decompilation’ and ‘reverse engineering’ are synonyms as the terms are used in [legislative history].<sup>22</sup>

The basis in the copyright act sect 4 is that a copyright holder cannot refuse another to use his work in a way which results in new and independent works. The copyright act sect 39i authorises the reproduction of computer code and translate the form of the form when this is a condition to make available the information necessary for the functional interaction between a program being independently developed and other programs, if the act is made by a person authorised to use a copy of the program, and the information has not earlier been easily

---

<sup>20</sup> Reference is made to the report of the expert committee published in the government series of reports, NOU – NOU 1983:35 *Endringer i åndsverksloven m.v. (Amendments in the copyright act etc)*, page 63, first column.

<sup>21</sup> Reference is made to the government bill to the Parliament, Ot prp no 84 (1991-92) *Om lov om endringer i lov 12 mai 1961 nr 2 om opphavsrett til åndsverk m.v. og enkelte andre lover som følge av EØS-avtalen* (*On an act amending the act of 12 May 1961 no 2 on copyright protection etc and certain other acts as a consequence of the EEA-agreement*) sect 3.4.6.3.

<sup>22</sup> Reference is made to Ot prp no 84 (1991-92), see preceding note.

available and the act is limited to the parts of the original program which is necessary to establish functional interactivity.

In the expert report made available in the extract before the court, it is stated page 41:

‘The method which apparently most frequently is related to reverse engineering is what is termed decompilation of the object code of a computer program. This is a process which attempts reformulate the object code to something approaching the source code on a higher level. One identifies the individual instructions in the program and assembles these to a functional description on a higher level. There is no secure method to arrive at a detailed representation of the source code of the original program, but one will acquire knowledge of the principles on which the design for the program are based. The work of reforming the actual machine instructions in the object code to a representation of source code may be considered identical to the part of reverse engineering we have chosen to term reconstruction of design.’

The appellate court bases its argument on the fact that what was done by ‘the nomad’ was a reverse engineering of the algorithm and the play keys. Using the information gained from the Xing player and the authentication code of Fawcus, he was able to create a new program and establish a functional interaction with the DVD. Information was not available to him from other sources. A possible license from DVD CCA implied secrecy with respect to the play keys *etc*, and according to the philosophy of open source code in the LiVid community it was impossible to sign such a promise of secrecy. The program developed does not in any extensive way correspond to the original, and the copyright to the original program is therefore not infringed. If ‘the nomad’ did more than what was necessary to establish functional interaction, has not been investigated. One must therefore base the argument on these conditions not having been violated. The fact that he used the authentication code of Fawcus is in any case an argument in favour of only the necessary parts from the Xing player was used. It is not certain that ‘the nomad’ had lawful access to the program for performing the movies from which the data was extracted. This issue is discussed in further details below. But it is the actions of [A] which is the issue in this case, and he did not have information of the possibility that ‘the nomad’ did not own a legal copy of the Xing player until 4 November 1999. At this time DeCSS had been available on the Internet since 6 October 1999. The code had by mistake been published, and it must be presumed that the program was known in the community especially interested in such issues, for instance the LiVid community.

The prosecution has claimed that the decompilation was of an illegal copy. This is an infringement of the copyright act. The evidence for the copy of the Xing player being illegal is two statements in the IRC log. ‘The nomad’ states for instance 4 November 1999:

‘and therefore I prefer being anonymous, I do not own a legal copy of xingdvd.’

The appellate court cannot find that the prosecution’s burden of proof is satisfied with respect to the ownership of the Xing player. Reference is made to the fact that the program of which the ownership is disputed, is a program for performing DVD movies for a PC, and these programs are not expensive to purchase. There is therefore not much reason to experiment on a pirate copy. Furthermore, several passages in the chat logs, for instance the log of 3 November 2000, states that ‘the nomad’ did not know the rules for reverse engineering. From what has been mentioned, ‘the nomad’ is German, and it would have been relatively easy to have him examined by German police on behalf of Økokrim if the data gained from the chat log was considered to be of decisive importance.

The appellate court holds, as stated above, that this issue is not critical for the criminal liability of [A], as the information, if it is correct, only become known a month after [A] had published DeCSS on the Internet.

According to the opinion of the appellate court, it can hardly be required that [A], at that time 15 years of age, should have made himself familiar with the provisions of the copyright act with respect to reverse engineering. The appellate court makes reference to the fact that he himself had not done this operation, among other things because he did not have the necessary knowledge. He had, according to the view of the appellate court, no cause to explore the provisions governing this issue. That his knowledge in this respect was very limited is apparent, among other things, from a chat log between him and Brian Demsky of 8 October 1999. He is then asked by Demsky if he had any idea of the legality of the reverse engineering. His response is, 'as in where? as if he did this in a country where this is permitted?' Brian Demsky explains that he means whether the reverse engineering is sufficient different not to infringe copyright acts. The response of [A] is, 'Sufficiently different.'

The appellate court then must address the issue of whether accessing the play keys themselves was illegal. The prosecution has claimed that these are data for the administration of rights which were not considered available for access by the consumer. The appellate court cannot see that this part of what is stored on the DVD enjoys any special protection. The key storage represent the protection, and what is considered illegal according to the criminal code sect 145 second paragraph must, as is the view of the appellate court, be related to accessing the movie as such. [A] has only examined whether the keys of 'the nomad's code worked with respect to certain movies. The rest of the keys are not exploited. In addition has, as mentioned above, Frank Stevenson developed and published a program which makes knowledge of the keys completely superfluous.

The court also wants to state that the fact that the protection scheme was compromised more is caused by it being insufficient rather than the attempts being especially intensive. Stevenson characterised the security of the system as very low, and it is evident that such a system is more prone to attacks than systems which initially present themselves as robust.

The appellate court therefore bases its decision on the fact that when [A] programmed the user interface to DeCSS, he had no reason to believe that the reverse engineering or decompilation of the 'nomad' was illegal. The appellate court concludes on this basis that access to the data cannot be construed as illegal.

The last two issues which have to be addressed by the appellate court is if [A] can be punished for contribution or attempt to contribution to the use by others of the program DeCSS.

The appellate court holds the opinion, as did the first instance court, that there has not been offered any evidence for anybody else having used DeCSS for illegally acquired DVD movies. [A] can not be convicted for contribution for the use of the program.

The issue is then whether he can be convicted for attempt for contribution by publishing a program making it possible for others to gain illegal access to decrypted DVD movies.

As the first instance court, the appellate court refers to Erling Joahannes Husabø<sup>23</sup> where the author bases his argument on the hypothetical: 'Almost anything can be used for a crime. Some things even imply a possibility for such use. But it is the unanimous view that criminal liability is excluded for both producer and seller.' The author refers for instance to the trade in weapons or medication as examples of a permitted risk. As long as the goods serves a legal

---

<sup>23</sup> Reference is made to the monograph *Straffansvarets perefieri – Medvirkning, forsøk, førebuing (The periphery of criminal liability – Contribution, attempt, preparation)* 1999 page 100.

purpose, the problem is not as much to argue for criminal liability as finding good reasons for that a sale to a third party may be the basis for a contributory liability.

The appellate court has above argued that the objective of [A] to make DeCSS available on the Internet was to contribute towards the development of a player for Linux. According to the philosophy of open publishing others might test the program and make it subject to further development. There are few indications for him by the publishing to have wanted to make it easier for others to publish or distribute DVD movies, though he obviously must have been aware of the possibility of the program being misused. Distribution and copying were, as discussed above, not practical in 1999. In addition reference is made to chat logs, as mentioned above, stating that [A] did not favour pirate copying. The appellate court cannot after this find that there has been offered evidence that by making DeCSS available on the Internet, he has contributed to the pirate copying of feature movies by others. That the program may be misused does not invalidate this assessment.

The appeal is after this rejected.

The issue of confiscation and expenditure for the proceedings are therefore not relevant.

The decision is unanimous.

*Decision:*

The appeal is rejected.

*[At this time it is not known whether the decision will be appealed to the Supreme Court. in that case, the Supreme Court's Appellate Committee will decide whether such an appeal will be permitted.]*