ALAI 2001 National Reports
Session IC
Italy

Anti Circumvention Protection Outside Copyright

(General Reporter: Prof. Séverine Dusollier)

1. Types of Circumvention

Are any of the following acts prohibited under some legal regime in your country, and if so, please specify which regime:

a. Gaining access to a technologically protected computer system or to protected material without authorization?

Yes.
- Article 615*ter* of the Italian Criminal Code ("Abusive access to an information or telecommunication system") provides that *"whomever illegally introduces him/herself into an information or telecommunication system protected by security measures or remains in such system against the express or tacit will of the person having the right to exclude him/her, is punished with the imprisonment up to 3 years.*
The punishment is the imprisonment from 1 to 5 years:
1. if the crime is committed by a public officer or by anyone in charge of a public service, with abuse of powers or with breach of duties related to the function or service, or by anyone acting, even abusively, as private investigator, or by abusing of his/her quality of operator of the system;
2. if the guilty person in order to commit the crime uses violence over things or individuals or if he/she clearly carries weapons;
3. if the fact entails the destruction or the damage of the system or the partial or total interruption of its functioning, or the destruction or damage of the data, the information or the programs contained therein.
In the event that the facts described at the first and second paragraphs above concern information or telecommunication systems having a military interest or related to public order or public security or health or public protection or anyway bearing a public interest, the punishment is, respectively, the imprisonment from 1 to 5 years and from 3 to 8 years.
In the case foreseen by paragraph 1 the crime is punishable under claim of the offended person; in the other cases the action is started ex officio".

- Article 615*quater* of the Italian Criminal Code ("Abusive possession and dissemination of access codes to information or telecommunication systems") provides that "*whomever, with the purpose of gaining a profit for him/herself or others or to cause a damage to others, abusively obtains, reproduces, disseminates, communicates or gives codes, keywords or other means suitable to access an information or telecommunication system, protected by security measures, or in any way provides information or instruction suitable for such aim, is punished with the imprisonment up to 1 year and with a fine up to Itl. 10.000.000.*
The punishment is the imprisonment from 1 to 2 years and the fine from Itl.10.000.000 to Itl. 20.000.000 upon occurrence of any of the circumstances indicated under points 1 and 2 of paragraph 4 of art. 617quater of the Italian Criminal Code" (punishing the interception, impediment or illicit interruption of computer communications, among others, in the cases where the crime is committed:
"1. to the damage of an information or telecommunication system used by the State or other public body or by a business in charge of public services or services of public utility;

2. by a public officer or by anyone in charge of a public service, with abuse of powers or with breach of duties related to the function or service, or with abuse of his/her quality of operator of the system").[1]

b. Receiving protected data or material without authorization or without paying the due remuneration?

Yes, by the above mentioned article 615*quater* of the Italian Criminal Code.

To this purpose, the Italian Supreme Court has rendered a decision[2] on July 2, 1998, by which it has interpreted this article specifying that its provision is also applicable to the commercial distribution of "Pic-Cards" containing the necessary codes for the functioning of decoding machines of encoded television signals.

c. Gaining access to a technologically protected computer system or to protected material by supplying a false name or password?

Yes, although not expressly foreseen by any of the above mentioned articles 615*ter* and 615*quater* of the Italian Criminal Code, we believe that this hypothesis should fall within the types of circumvention prohibited by the said rules.

d. Gaining access to a technologically protected computer system or to protected material by supplying a false Internet protocol (i.p.) address?

Yes, although not expressly foreseen by any of the above mentioned articles 615*ter* and 615*quater* of the Italian Criminal Code, we believe that this hypothesis should fall within the types of circumvention prohibited by the said rules.

e. Gaining access to technologically protected material by supplying false payment information?

Yes, although not expressly foreseen by any of the above mentioned articles 615*ter* and 615*quater* of the Italian Criminal Code, we believe that this hypothesis should fall within the types of circumvention prohibited by the said rules.

f. Decrypting without authorization encrypted content?

Yes, although not expressly foreseen by any of the above mentioned articles 615*ter* and 615*quater* of the Italian Criminal Code, we believe that this hypothesis should fall within the types of circumvention prohibited by the said rules.

g. Overriding a limit on the number of simultaneous users allowed access or on the allowed time of access?

Yes, although not expressly foreseen by any of the above mentioned articles 615*ter* and 615*quater* of the Italian Criminal Code, we believe that this hypothesis should fall within the types of circumvention prohibited by the said rules.

h. Overriding a limit on the number of copies an authorized user is permitted to make, or a technologically enforced prohibition against making *any* copies?

[1] Both translations are informal and have been made by us.
[2] n° 4398/98

Yes, although not expressly foreseen by any of the above mentioned articles 615*ter* and 615*quater* of the Italian Criminal Code, we believe that this hypothesis should fall within the types of circumvention prohibited by the said rules.

2. General tort law rules of direct or secondary liability

a. Under your country's general tort law principles, could a person be held liable for having engaged in an act of circumvention or for having manufactured or distributed a circumvention device? What would be the conditions for liability?

As a general rule, art. 2043 of the Italian Civil Code states that "any intentional or faulty fact that causes to others an unjust damage, obliges those who committed it to repair the damage".

b. Has your country's case law already applied tort law to prohibit or to enjoin the act of circumventing or the manufacture or distribution of a circumvention device? Are knowledge or intent required? How have knowledge or intent been defined? Is the liability of manufacturers and distributors of devices direct, or based on secondary liability (contributory or vicarious)?

We are not aware of any such decision.

c. If general tort principles may apply in your country to prevent the act of circumventing, or the supplying of circumvention devices, are there exceptions to the scope of the prohibitions?

No, provided that the violation is due to intention or fault and causes damages to the right-owner.

d. Under what circumstances might resort to technological measures to block access be considered in your country an "abuse of right"?

We are not aware of any precedent relevant to this issue.

3. Broadcasting law, cable and satellite regulations, protection of encrypted services or broadcasts, protection of conditional access services

a. Are encrypted services or broadcasts (e.g. pay-TV signals, etc.) legally protected in your country? Is the regulation civil, administrative, criminal or public? What is the rationale for this regulation?

Yes, by a series of civil, administrative and criminal regulations.

In such legislation, is the decryption, descrambling or any other form of unauthorized interception of encrypted services or broadcasts prohibited? Under what conditions? What are the rationale and purpose for such prohibition? What are the services or programs at issue? Is protection available only if the broadcast or transmission requires payment? (i.e., no protection for free broadcasts of transmissions?) Who may bring a claim? What remedies are available?

See below, under b.

b. Is the distribution of devices that enable or facilitate circumvention illicit? What are the criteria for considering a device to be illicit? For example, is there a requirement of knowledge or intent to engage in or facilitate illicit circumvention? What commercial/private activities related to that device are prohibited (manufacture, distribution, sale, possession, etc.)? How does the law address devices that potentially have licit and illicit purposes? Who may bring a claim? What remedies are available?

Italian Law n° 422 of October 27, 1993 ("Urgent provisions concerning the teleradiobroadcasting system") has confirmed into law the urgent Decree n° 323 of August 27, 1993, article 11 of which

states that "encoded transmissions referred to in previous paragraph 1[3] shall in any case be protected according to art. *171bis*" of the Italian Copyright Law (prohibiting the unlawful duplication, import, distribution, sale or possession of computer programs, with imprisonment from 3 months to 3 years and a fine from Itl. 1.000.000 to Itl. 10.000.000).

Moreover, the Legislative Decree of November 15, 2000 (implementing the Directive n° 98/84 EC of the European Parliament and of the Council of November 20, 1998, on the legal protection of services based on, or consisting of, conditional access) prohibits (art. 4) the manufacture, import, distribution, sale rental or possession, as well as the installation, maintenance, or replacement for commercial purposes of any equipment or software designed to give unauthorized access to a protected service, punishing the crime (art. 6) with a fine from Itl.10.000.000 to Itl. 50.000.000 and the seizure of the illicit material.

c. Are there circumstances in which circumvention or decryption is authorized or exempted from the prohibition? How have courts in your country applied the prohibitions (or exceptions) to circumventing technological protections for broadcasts and transmissions?

No.

d. Do you consider these legal provisions as adequate and effective?

Yes.

e. Conditional Access:

In The European Union, a directive of 1998 protects conditional access services, defined as "services provided against remuneration and on the basis of conditional access," whereas "Conditional Access" means "*any technical measure and/or arrangement whereby access to the service in an intelligible form is made conditional upon prior individual authorization."* Protected services could be television and radio broadcasting services as well as Information Society Services, e.g. video or audio-on-demand, electronic publishing, on-line access to a database and a wide range or other on-line services.

1. Is there a similar protection in your country? In which legal regime (broadcasting law or other)?

If yes, what is the rationale of the protection? Which services are covered? What are the requirements for protection? Is conditional access defined on the basis of a requirement of payment for the transmission? Is the circumvention of the conditional access measure and/or the circumvention device prohibited? Which activities related to circumvention devices are prohibited (sale, manufacture, possession, etc…)?

The Directive has been fully implemented in Italy, which therefore applies the same regime of protection foreseen therein.

2. The European Directive also covers the so-called "Information Society services", i.e. services provided at distance upon individual request from the recipient of the service. Does your legislation on conditional access concern information society services as well? In other words, could your conditional access legislation be applied to services provided through the Internet or other networks?

The Directive has been fully implemented in Italy, which therefore applies the same regime of protection foreseen therein.

[3] i.e. effected by cable or satellite

4. Telecommunications Law

a. Telecommunications law sometimes prohibits unauthorized interception of any wire or electronic communication. This could serve as a basis for a claim against decryption or any other unauthorized means of getting access to data when transmitted over telecommunication networks. Does your country's telecommunications law include such a prohibition? If so,

1. Which acts are concerned (interception, disclosure, unauthorized access, reception, etc.)? Does the law cover interception devices as well?
2. Does the content have to be encrypted or otherwise protected so as to benefit from protection?
3. What are the circumstances where interception is authorized or where interception devices are legitimate (e.g., when they comply with some technical standards)?
4. Who may bring a claim? What remedies are available?

We are not aware of any such provision.

b. Telecommunications law might also impose mandatory technical standards to be applied to telecommunication reception devices. This could lead to prohibiting devices enabling the unauthorized reception of communications. What about the telecommunications law in your country?

The Italian legislation complies with the principle of promoting technical standard set forth in the Directive n° 95/47/EC of the European Parliament and of the Council of October 24, 1995, on the use of standards for the transmission of television signals, that has been implemented in Italy with the Legislative Decree n° 191 of May 17, 1999. Art. 10 of the said Decree prohibits the "import, distribution in any form or installation" of devices not complying with the standard set forth therein, subject to a fine from Itl.8.000.000 to Itl. 48.000.000 and the payment of an amount from Itl. 40.000 to Itl. 240.000 for each device.

5. Computer crime

a. In your country, is there legislation related to computer crime? Can circumvention of technological measures and/or unauthorized access to computer systems, networks or data be prosecuted under such statutes? What is the rationale of criminalizing such offenses?

Computer crime has been the object of a specific regulation (Law n° 547 o December 23, 1993), that has introduced several new provisions in the Italian Criminal Code, among which specifically articles 615*ter* and 615*quater* mentioned under previous question 1 a, in order to combat the phenomenon.

b. What is the definition of the offense? Is the way of getting unauthorized access defined: e.g. providing a false password, decrypting, cracking the technical protection, etc.?

Please refer to the answers given under previous question 1.

c. Can the manufacture or distribution of devices enabling the carrying out of these offenses be prosecuted as well (such devices are sometimes called 'hacker tools')? If not, could the seller or manufacturer of circumvention devices be prosecuted as an accomplice? What are the penalties for the offense?

Please refer to the answers given under previous question 1.

d. Is knowledge or malicious intent required to constitute the violation?

Yes. In both crimes of abusive access (art. 615*ter*) and abusive possession and dissemination of access codes (art. 615*quater*, where a "*purpose of gaining a profit*" is expressly foreseen).

e. Has computer crime legislation already been applied by your country's courts to the unauthorized access to protected information or transmissions, or to the circumvention of technological protection measures?

Please refer to the answers given under previous question 1 b.

f. In the absence of specific provisions on computer crime, could unauthorized access and/or the circumvention of technological measures be considered to violate other penal laws (e.g., offences such as theft, fraud, breaking and entering, forgery, etc.)? Are there some examples in the case law?

Computer crimes violate specifically dedicated provisions of the Italian Criminal Code.

6. Unfair Competition law or unfair commercial practices

a. In your country, in the absence of specific prohibitions on circumvention or unauthorized access, has the distribution of circumvention devices or descramblers been prohibited through the application of unfair competition law? Under what circumstances?

We are not aware of any such decision.

b. What are the advantages, disadvantages and boundaries of the recourse to unfair competition law as far as circumvention activities or devices are concerned? Do you consider this protection as sufficient and effective?

7. Protection of technological measures as such

Technical means of protection might be in themselves protected by a proprietary right, e.g. by a copyright (for instance if the technological measure consists of software), patent or trade secrets. In such a case, circumventing the software or the technical system or developing circumvention devices could effect an unauthorized reproduction of the software (namely by reverse engineering) or a disclosure of the trade secret.

a. In your country, what legal regime of exclusive or related rights might apply to the technological measure? Under what conditions? Do you know any case law in that field?
b. What exceptions related to these legal regimes could be applied to legitimate the circumvention act or device?

It is worth mentioning that the Council Directive n° 91/250/EEC of May 14, 1991, on the legal protection of computer programs has been implemented in Italy with amendment of the Italian Copyright Law, that now contains a whole new section dedicated to this issue (artt. 64*bis*, 64*ter* and 64*quater*).

Art. 64*bis* reflects art.4 of the Directive[4], art. 64*ter* reflects art. 5 of the Directive[5] and art. 64*quater* reflects art. 6 of the Directive[6]. The latter provision could be relevant to this issued, as the "decompilation" could be intended as a legitimate form of circumvention.

8. Other protections

a. Can you think of any other means of protecting technological measures against circumvention in your country? In which legal areas and by which mechanisms (e.g., privacy law, property right, "trespass", "conversion," …)?

---

[4] "***Article 4 Restricted Acts:*** *Subject to the provisions of Articles 5 and 6, the exclusive rights of the rightholder within the meaning of Article 2, shall include the right to do or to authorize:*

a) the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole. Insofar as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorization by the rightholder;

b) the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program;

c) *any form of distribution to the public, including the rental, of the original computer program or of copies thereof. The first sale in the Community of a copy of a program by the rightholder or with his consent shall exhaust the distribution right within the Community of that copy, with the exception of the right to control further rental of the program or a copy thereof."*

[5] "***Article 5 Exceptions to the restricted acts:***

1. In the absence of specific contractual provisions, the acts referred to in Article 4 (a) and (b) shall not require authorization by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.

2. The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract insofar as it is necessary for that use.

3. The person having a right to use a copy of a computer program shall be entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do."

[6] "***Article 6 Decompilation****:*

1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

(a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to do so;

(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and

(c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.

2. The provisions of paragraph 1 shall not permit the information obtained through its application:

(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or

(c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the right holder's legitimate interests or conflicts with a normal exploitation of the computer program."

b. In particular, do you think that, in your country, contract law can offer an effective prohibition against circumvention?

1. For example, a contract obliging each user not to circumvent can be embedded in the technological measure itself when it enables the on-line licensing of or access to transmissions (including content). Would such a contract be enforceable in your country?

   Yes.

2. Or contracts might be negotiated between content providers and the computer or consumer electronic manufacture industries in order to oblige them either to design devices that answer to technological measures or not to develop devices that are able to circumvent them. Are such negotiations in progress in your country?

   We are not aware of any such negotiation.

9. Limitations, exceptions, fundamental rights, third parties' and public interest

a. Are there any general limiting principles that could apply to the various legal regimes we have addressed in this report (e.g. freedom of expression, freedom of information, public interest, consumer protection, abuse of right, etc.)?

   No.

b. What are the concerns of computer and consumer electronics industries related to prohibitions of circumvention devices? Have these concerns been taken into account in the legal provisions addressed above?

10. Potential application of the protections surveyed in Questions 1-9 to copyrighted works

a. In your country, could copyright holders avail themselves of some or all of these extra-copyright legal provisions or mechanisms, either to prevent the act of circumvention of technological measures, or to prohibit trafficking in circumvention devices? If so, which ones?

   Yes. All of them.

b. Could the alternative means of protection for technological measures available in your country be added or used simultaneously with copyright-related anti-circumvention provisions?

c. What would be the pros and cons of recourse to extra-copyright protections against circumvention of access to copyrighted works or circumvention of technological protections of rights of the author? Do these protections call for reassessment of the need for copyright-specific protections?

d. If recourse to extra-copyright protections is available, could your country implement the WIPO treaty obligations without copyright-specific anti-circumvention legislation? In your view, would this be a desirable approach? If not, to what discrepancies or failures in the existing law would copyright-related anti-circumvention provisions need to respond?

   [No responses provided for 10 b-d.]

Any other observations?

No.

Milan, April 9, 2001

Avv. Alberto Pojaghi