CAPÍTULO II

UNA PROTECCIÓN POR LAS VÍAS COMUNES SIN EFICACIA REAL

CAPÍTULO II

UNA PROTECCIÓN POR LAS VÍAS COMUNES SIN EFICACIA REAL

1. ELEMENTOS A CONSIDERAR

Frente al peligro que representa para los productores y usuarios de buena fe de programas el uso fraudulento de esos productos, varios tipos de reacción son previsibles, los cuales podemos reagrupar en dos áreas bien definidas: la técnica y la jurídica. En cuanto a la primera, se caracteriza por ser muy costosa y compleja. Por otra parte, los métodos jurídicos "clásicos", como aquellos que utilizan las técnicas comunes del derecho al ser considerados como apropiados, se presentan en el momento de la apreciación de resultados, como desprovistos de eficacia real frente al problema. La comprobación de esta doble insuficiencia la abordamos a continuación:

2. INSUFICIENCIA DE LA PROTECCIÓN TÉCNICA

La protección técnica consiste en un resguardo en secreto del programa. El secreto puede ser obtenido reduciendo técnicamente la accesibilidad o la utilización de los programas. Esas técnicas son generalmente onerosas y por momentos ineficaces; sin embargo, dadas las circunstancias, ninguna firma puede privarse de usar esos medios de resguardo.[15]

Es entonces normal que el proveedor tome medidas de protección que le permitan, por ejemplo, contabilizar la frecuencia de uso de su programa y prever, al final de ese período, la destrucción del mismo. Por otra parte, el proveedor tomará todas las precauciones necesarias para que su cliente se comprometa a garantizar las faltas de sus empleados, a fin de evitar la comunicación de su programa a terceros deseosos de la apropiación del secreto.

---

[15] Consultar, en ese sentido, Afnor, *Securité informatique protection des donneés*, Ed. Eyrrolles, 1983, p. 183; A Bensoussan y M. Salvator, *Risques. Informatiques: Parades techniques et juridiques*, Ed. des Parques 1983. L. Kraus y A. Mc. Gahan, *Computer Fraud*, Ed. Prentice Hall, 1979, y Boby Traps That Catch Deads beats, *Bussines Week*, 31 de mayo de 1982, p. 70.

La criptografía y el borrado interno son dos medios importantes dentro de esta protección técnica, por lo que serán objeto de un tratamiento a continuación.

A. *Los métodos de criptografía*

Entre los diversos sistemas de protección técnica destinados a asegurar las necesidades de seguridad y control de la información en el caso particular de los programas de cómputo, encontramos a la criptografía como el sistema más interesante y potencialmente eficaz. De hecho, sólo algunas compañías practican una política de seguridad de este orden en virtud de los altos costos que representa.

Para tratar de comprender esta nueva técnica, hay que mencionar que la criptografía es la ciencia que transcribe las informaciones en forma secreta; forma incomprensible para toda persona que no sea el usuario o destinatario. El "descriptaje", a su vez, es la ciencia cuyo objeto es el descifrado de las informaciones secretas o codificadas sin el conocimiento previo del código, del método o la clave del código. La criptografía es la amalgama de esas dos ciencias.

Expuesto lo anterior, es conveniente mencionar que la protección deriva entonces de la criptografía normalmente utilizada para prevenir y controlar el abuso y para autenticar las fuentes y las informaciones que pueden estar comprendidas. La criptografía consiste, por tanto, en "criptar" los programas por un sistema de codificación sofisticado que emplea una o varias claves, conjunto de caracteres que transforman un método general o un algoritmo específico en informaciones codificadas, a efecto de que si el competidor pirata o "enemigo" conoce el algoritmo no le sea de provecho, pues deberá conocer, también, la clave, la cual podrá ser cambiada y representar consecuentemente un nuevo obstáculo para aquel que quiera tener acceso al sistema. Estos métodos son por momentos tan eficaces que el algoritmo codificado puede puede ser objeto de una publicación o ser conocido sin representar problema alguno.[16]

Las diferencias entre los diversos métodos de criptografía residen en que la transformación no utiliza el procedimiento de operaciones lineales, es decir, de adición o de multiplicación, pero pone en práctica el estudio reciente de las funciones no lineales. Es así como la investigación del algoritmo necesario al "descriptaje" es imposible en un período razonable, aun con una computadora. Es evidente que la evolución

[16] La compañía IBM ha concebido y comercializado un sistema de codificación denominado *DES,* considerado inviolable; empero, ciertas sociedades como la Bell Telephone Laboratories, Inc., no piensan usarlo dada su complejidad. Este sistema se usa bajo la forma de microcomputadoras colocadas en los órganos de entrada y salida o en la terminal.

de los materiales reducirá sensiblemente el tiempo necesario a la investigación de los algoritmos y convertirá en vulnerables los sistemas protegidos.

Ahora, la introducción del uso del "criptaje" ofrece varios riesgos: la pérdida de las claves del "criptaje" y, consecuentemente, la de las informaciones; el "robo" de las claves; el mal funcionamiento de los aparatos de criptaje o aun su ineficacia; la imposibilidad de introducir nuevas claves en un tiempo deseado, etcétera.

Por otra parte, los sistemas actuales tienen en común un punto débil, y es que la clave puede estar a la disposición de varios usuarios, incrementando los riesgos, ya que si la clave es divulgada el sistema se torna accesible. Así, aun si la criptografía reduce en cierta medida la vulnerabilidad de los sistemas, es asimismo generadora de vulnerabilidad.

En cuanto a los costos, si el computador "permite" el descriptaje de los códigos más herméticos, resultará muy caro y exigirá tiempo para el perfeccionamiento.

Queda por determinar si el riesgo para una empresa, en caso de divulgación de un programa, amerita o no invertir una suma importante en el criptaje del mismo, y por otra parte, aquel que desea hacerse de un programa protegido, si el precio exigido para el descriptaje vale la pena ser cubierto. En toda hipótesis hay que tener en cuenta que esos costos son considerablemente afectados por la revolución de semiconductores y tendientes a disminuir en lo futuro.

Podemos aventurar que de aquí a diez años potentes sistemas criptográficos que utilicen claves automáticas podrán ser productos masivos a costos razonables.[17] De esta forma, actualmente y en espera de una protección por medios jurídicos convincentes, numerosas empresas escogerán, a pesar de todo, recurrir a un método como el criptaje, bajo la idea de que los costos a absorber serán menos onerosos que los que provocan el pillaje y la piratería.

B. *Los métodos del borrado interno*

Para evitar la piratería de sus programas, algunas empresas y programadores independientes han introducido lo que podemos designar como los métodos de borrado interno. Empresas de microcomputadoras como la American Integrity Systems Incorporated (AIS), con sede en Santa Ana, California, utilizan esos procedimientos para proteger a sus distribuidores de compradores de mala fe y para impedir a los

[17] Ver. D. Parker, *Fighting Computer Crime*, Nueva York, Scribners, 1983, pp. 310 y siguientes, y M. Dortonzos, *MIT Comunites Seek Cryptography Policy Science*, vol. 22, 13 de marzo de 1981.

clientes el "copiar" sus programas en otros sistemas. La AIS utiliza el método del reloj interno en sus programas, mediante un conjunto de instrucciones por las cuales estos dejan de funcionar pasados treinta días.

Si el programa es pagado por adelantado se entrega con un código, especie de instrucciones adicionales listas a evitar el funcionamiento de "bloqueo", que de otra forma sería imposible de detener. De todos modos, aun cuando el cliente no pague con anticipación, deberá recibir del vendedor ese mismo código, ya sea por teléfono, visita expresa u otra manera, a falta de la cual el sistema dejará de funcionar en el tiempo fijado.[18]

La misma AIS dispone de otro método con un sistema que detiene el proceso informático después que una cierta frecuencia se repite en diversas ocasiones. El usuario deberá obligadamente consultar a su programador o proveedor para que el sistema funcione de nuevo. Los usuarios no deberán saber por qué los sistemas dejan de funcionar; la situación se les presenta como un error del sistema de instrucciones que les indica: "consulte a su distribuidor".[19] Es menester agregar que la AIS, para protegerse contra la piratería de sus programas y con un fin de control, atribuye un número de registro a cada cliente que adquiere un programa específico.[20]

Por otra parte, la compañía Grid Systems Corporation de Mountain View, California, otra empresa de microcomputadoras, experimenta dispositivos listos a ser introducidos en los sistemas, consistentes en un reloj calendario presentado bajo la forma de un circuito integrado al equipo, que fija una fecha de expiración en el funcionamiento de los programas. Si el pago de estos últimos no se efectúa en los treinta días siguientes a la fecha fijada, el dispositivo impedirá automáticamente que el sistema continúe funcionando. Luego de ser prevenido, el cliente promete pagar normalmente, pero si ello no llegara a suceder, el dispositivo accionará descomponiendo los sistemas de calefacción, de aire acondicionado y los que controlan la temperatura del agua.

Asimismo, el dispositivo impide la duplicación o el copiado impropio del programa por un mecanismo de codificación de pistas, realizado por esta empresa, y que en caso de necesidad da lugar al borrado del programa en cuestión.[21]

---

[18] Ver el artículo "Boody Traps that catch Deadbeats", *Bussiness Week*, 31 de marzo de 1982, p. 70.

[19] *Ibid.*

[20] *Ibid.*

[21] *Ibid.*

El uso de estos dispositivos, si bien es cierto que ayuda a limitar la piratería, presenta a su vez el inconveniente de que un programador descontento pueda sabotear el programa luego de que este empleado deje la empresa. Por esta razón Donn Parker, presidente consultor de sistemas de la compañía SRL International, en Menlo Park, California, habla de los posibles sabotajes a los programas como un verdadero delito informático, preconizando para fines de protección los consejos de seguridad siguientes:[22]

1) Establecer un código de conducta especificando aquello que constituye o no una actividad autorizada, haciendo mención de las leyes que permitan la persecución en caso de delito.
2) Organizar reuniones especiales con el personal que presente problemas con la empresa.
3) Utilizar "contactos" dispersos en la empresa.
4) Recurrir a un sistema individual de funciones, de verificación y balances para vigilar continuamente al personal.
5) Desarrollar políticas para el personal incorporando datos varios y entrevistas susceptibles de mejorar las relaciones o enviar al empleado a vacacionar por dos semanas para "separarlo" de los demás y provocar un cambio de actitud más positivo en favor de la empresa.

Sin embargo, lo anterior conforma sólo un paliativo. La protección (técnica) perfecta no existe. Lo cierto es que la protección de los programas no puede resolverse utilizando sólo estos medios técnicos. Hay que considerar necesariamente al derecho, aun si en primera instancia pueda derivarse una comprobación de insuficiencia.

3. Insuficiencia de la protección del derecho clásico

Es indudable que en el ámbito informático y en el caso de la programación de computadoras, los contratos han jugado y juegan un papel muy importante para la negociación y la difusión de los "productos-programas". Lógicamente, hay siempre (o debe haber siempre) cláusulas que prevean sanciones en casos de comportamientos contrarios a la economía misma del contrato. Pero es conveniente contemplar *dónde* el contrato no ofrece nada, o por lo menos, nada satisfactorio, hipótesis bien frecuente de imaginar.

---

[22] Contenidos en la obra de Donn B. Parker, *Crime by Computer*, Nueva York, Ed. Scribners, 1981.

A. *La protección por contrato*

El contrato es actualmente un medio importante en la protección de los programas.[23] Salvo alguna excepción, todo contrato referente a un programa (o materia gris) deberá, en efecto, hacer alusión a cláusulas que garanticen la seguridad de los datos, y prohibir el acceso a los mismos a toda persona no autorizada a:

—Obtener informaciones que "pertenezcan" al contratante (ya se trate de copia, duplicación de archivos o "robo" de programa.)

—Modificar las informaciones contenidas en un soporte magnético, o modificar su programa.

—Destruir informaciones, borrar el contenido de un disco o una banda magnética o escribir en una banda que contenga información.

—Utilizar los recursos de un sistema sin autorización.

—Explotar un programa donde el uso esté reservado por contrato.

—Conviene precisar que todos los agentes y personas que con motivo de la ejecución de un contrato tengan acceso a datos, o a programas que una empresa desee reservar en secreto, deberán comprometerse éstos a un régimen de confidencialidad en que los responsables estén constreñidos por escrito a destruir o borrar todas las "copias" que les sean dadas con motivo de la ejecución del contrato.

Existe igualmente interés en indicar en el contrato los datos y programas que presentan un carácter "sensible", a fin de que la atención del personal del proveedor se enfoque hacia las consecuencias que tendría la divulgación de esos datos al exterior de la empresa. Por ello es sumamente recomendable asegurarse que:

a) El personal que ejecutará el contrato ha sido notificado del carácter confidencial que presentan los datos y los programas en cuestión.

b) Que el contrato contiene una cláusula de "secreto profesional".

c) Que estas personas sean objeto de las mismas reglas de disciplina general aplicables al personal especial en materia de seguridad.

Por otra parte, el cliente puede exigir por la vía contractal y en ciertos casos, que el proveedor se comprometa a no divulgar la natura-

[23] Sobre los llamados "contratos informáticos", es decir, aquellos derivados del sector informático con motivo de las cláusulas de protección, ver particularmente: A. Lucas, "Los programmes d'ordinateur comme objets de droits intellectuals", *JCP,* 1982, I, 3081, núm. 165; *Actuel Informatique* 1983, núm. 60, p. 185; *La souplesse de la protection contractuelle;* H. de Champois, "La nature des contrats relatifs aux logiciel", *Bureaux de France,* 1983, núm. 183, p. 26; Isabelle de Lamberterie, *Les techniques contractuelles suscités par l'informatique,* París, CNRS, 1977; "Aspects contractuels des marchés de materiels informatique", *Dossier Organisation FNCA,* enero de 1978; *Purchasing Computers,* E.R., Cambridge Gower Press, 1977, y "Le contrat de logiciel, aspects juridiques et practiques", *Etude CXP,* núm. 60, 1980.

leza de las prestaciones efectuadas por su cuenta, así como no hacer ninguna referencia sobre él.[24]

Para exponer un ejemplo concreto, citamos la cláusula siguiente contenida en los contratos IBM intitulada "Mínimo: secreto profesional":[25]

1) Todos los colaboradores del proveedor están constreñidos por contrato al secreto profesional más absoluto sobre todas las informaciones a las cuales tengan acceso en el curso de la ejecución del contrato.

2) El proveedor se compromete a tomar todas las medidas necesarias para hacer respetar esas disposiciones por su personal.

3) El proveedor se compromete a no publicar y a no citar como referencia los trabajos efectuados para el cliente sin una autorización escrita de éste.

4) El cliente puede exigir, en el curso de ejecución del contrato, el reemplazamiento de un colaborador del proveedor por otro igualmente calificado sin mediar una explicación.

5) El proveedor se compromete a respetar el reglamento de seguridad y los procedimientos que son impuestos por el cliente a su propio personal que deberá tomar conocimiento previo.

6) La obligación de secreto no se aplica a las ideas generales a la concepción o los métodos técnicos particulares que nacen en el curso del estudio y perfeccionamiento del programa objeto del contrato, al igual que informaciones que sean de notoriedad pública.

Utilizar un programa previsto por un constructor (en IBM está bien precisada en los llamados contratos de "programas bajo licencia", aun si la expresión es sin duda jurídicamente inexacta) o por una sociedad de servicios, obliga a tomar las precauciones necesarias para que ese programa no sea utilizado más que en el cuadro del contrato con el proveedor, sin existir un duplicado utilizable por un tercero.

En la práctica los contratos de elaboración y de utilización estipulan, por un lado, que el programa contemplado en el contrato es propiedad de una de las dos partes, lo cual constituye una anticipación sobre la resolución del problema mayor que opone la protección de los programas, como es aquel de su reserva privativa,[26] y por otro lado, el que los participantes en la elaboración del progrma se comprometan a conservar el secreto.

---

[24] Ver sobre el particular la "Guide d'élaboration cahier des charges pour un appel d'offres de materiel et/ou de logiciel en informatique", Ministère de la Cooperation, Mai 1978; "Maintenance des systèmes d'informatique répartie", guide INFOREP, mayo 1979.

[25] Cláusula tipo introducida en los contratos informáticos IBM.

[26] Ver *infra* capítulo II.

Ilustra lo anterior el artículo 11 del "contrato de licencia" del programa IBM L 9500 1/6-10:

> En ningún momento, durante y después de la ejecución del presente contrato, el cliente podrá proveer o comunicar a ninguna persona salvo miembros de su personal o. de IBM todo programa bajo licencia y/o documentos opcionales y su contenido, particularmente los organigramas, bajo cualquier forma que sea, sin el consentimiento escrito y previo de IBM...

Podemos citar asimismo el artículo VII, 5o. del contrato de servicio Honeywell-Bull que prohíbe toda reproducción del programa y obliga al cliente a mantener en buen estado las menciones de propiedad de la firma sobre las máquinas, soporte de los programas y los programas mismos.[27]

El valor efectivo de las cláusulas de protección de estos contratos depende evidentemente del respeto de que sean objeto por las partes. Ahora, es menester mencionar que el carácter altamente sofisticado de la industria de programas no parece mostrar una "moral" similar,[28] lo que demuestra que la protección contractual no es la panacea.

El contrato es continuamente, sino siempre, la traducción de una relación de fuerzas, lo cual está lejos de permitir la emanación de una justa solución. El desequilibrio de las partes es un cúmulo de datos importantes, por tratarse de un desequilibrio que puede ser fuente de abusos evidentes.

El peligro de irregularidades no queda exento en el caso de cláusulas abusivas que podrían provocar la anulación del contrato. Sin llegar hasta este extremo, hay que considerar que los tribunales tienen a mal interpretar cláusulas deficientemente redactadas, contradictorias y confusas.

Pero el más grave peligro es que estos contratos son ajenos a un derecho objetivo, concebido como un todo. La economía contractual está totalmente desequilibrada, por lo que el contrato pierde todo interés. Si eso que imaginan las partes está sin relación con las soluciones de conjunto que permiten dar lugar al derecho positivo, esos contratos concebidos con referencia a un derecho real no reconocen ni siquiera el derecho objetivo,[29] conduciendo a aberraciones tan grandes como las de un contrato estructurado sin fundamentos jurídicos; por tanto, hay que buscar la solución más allá del derecho contractual.

---

[27] Artículos citados por J. Debetencourt, "La protection juridique des programmes d'ordinateurs", *Ing. Conseil*, 1972, pp. 11-18.

[28] Ver David Bender, "Trade Secret Protection for Software", *G. Washington Law Review*, 1970, p. 912.

[29] Ver *infra* capítulo II.

B. *La protección extracontractual*

Estos medios de protección extracontractuales no aseguran jamás a los creadores de un monopolio con respecto a terceros. En principio, el único medio para el autor de una creación de evitar la entrega a sus competidores es el de mantenerlo en secreto. Sin embargo, es imposible excluir la hipótesis de una violación del secreto. No estimarlo así sería muestra de ingenuidad en esta época donde la innovación es una necesidad vital y donde el espionaje industrial toma proporciones inquietantes, según lo hemos visto.

Por tanto, puesto que esta protección de hecho por la vía del secreto no puede considerarse como suficiente, hay que buscar una protección jurídica que brinde una consolidación.

Podemos imaginar esta protección en un derecho donde la primera función es de orden disuasivo: el derecho penal. Y trataremos de dar aplicabilidad a las disposiciones sobre la protección del secreto ya sea, según los Estados, calificado de secreto comercial o secreto de fábrica.

Asimismo, podemos imaginar y considerar también las vías clásicas del derecho civil y recurrir así, por ejemplo, a la acción de la competencia desleal que sabemos deriva del derecho de la responsabilidad.

C. *El derecho penal*

Se trata de estudiar aquí las técnicas del secreto. La sutil diferencia existente entre los secretos comerciales (figura americana) y los secretos de fabricación (conocidos en Francia bajo el nombre de secretos de fábrica) no impide considerar estas dos vías como el género de acciones análogas utilizables, por ejemplo, contra los exempleados de una empresa que comuniquen ciertos secretos de importancia, provocando con ello un grave perjuicio económico o de "desprestigio" a su antiguo empleador.[30]

En los Estados Unidos, el recurso a la figura del secreto comercial hace referencia a una obligación implícita que se desprende de la ley y recae particularmente sobre los antiguos empleados o socios comerciales.[31] Pero en el caso específico de la protección de programas, el recurso a esta noción aparece como una solución relativa en la medida

[30] Ver J. Dragne, "L'alternative: secret ou brevet", *Revue Francaise de Gestion*, Janvier 1980, p. 70 et J.M. Mousseron, "La strategie du secret," *Rvue Francaise de Gestion*, Janvier 1980, p. 82.

[31] Ver M. Scott, "Trade Secrets and Employment Agreements," *The Scott Report*, Dec. 1983 p. 1; D. Remer, *Legal Care for your software*, Nolo Press, Berkeley 1982, p. 61 et 173; Bender, *op. cit.*, Raysman, R. "Protection of Proprietary Software in the Computer Industry", *IP Jurimetric* 335 (1978), y P. Luccarelli "The Supremacy of Federal Copyright over State Secret Law for Copyrigthtable Computer Programs Marke with a Copyrigth Notice," *Computer L.J.*, 1981, Número 1, pp. 19-52.

en que los creadores de un programa desean que éste, una vez protegido, sea objeto de una difusión a gran escala, lo cual no es muy compatible con la hipótesis del secreto comercial.

En Francia, el recurso al derecho penal es frecuentemente presentado como una solución eficaz. El tenor del artículo 418 del Código Penal que contempla el caso de violación de los secretos de fábrica y que prevé una sanción para los "directores, comisionados y obreros de una fábrica, que comuniquen los secretos de la fábrica donde estén empleados", es luego mostrado como "secretos empresariales ordinarios",[32] que bien puede objetarse como en el caso del secreto en los Estados Unidos. Sin embargo, hay que hacer notar que el artículo 418 del Código Penal francés no parece aplicable a los programas. En efecto, una interpretación de jurisprudencia discutible reenvía los "secretos de fábrica" aludidos en el Código Penal a los "secretos de fabricación".[33]

Ahora, si los programas no son una creación tan abstracta como la afirma la ley francesa y más ampliamente el derecho europeo sobre las patentes, no puede ser todo esto considerado normalmente como un proceso de fabricación, salvo quizá para ciertos programas de explotación si los tenemos como elementos indisociables del proceso general de fabricación. Invariablemente, una decisión reciente[34] por primera vez ha asimilado a los programas con un secreto de fábrica que hace valer el texto legalmente examinado; sin embargo, la decisión está bien aislada por la ausencia de otras decisiones sobre el particular.

Una tendencia favorable a tal régimen de protección es seguida en numerosos países, particularmente anglosajones y europeos, y la misma considera que una acción penal podría disminuir la divulgación intencional (o aun fortuita) de las informaciones de valor irrefutable contenidas en los programas de cómputo, lo que se ha convertido en gran problema, especialmente en las empresas.[35]

No es convincente el recurso al secreto aun reafirmado por la vía penal. ¿Podemos esperar más de la vía civil?

---

[32] Fabre, "Embauchage d'ourvriers pour le compte de étranger, Revelation de secrets de fabrique", *JCL. Penal*, arts. 417-418, y P. Mathely, "Le droit francaise des brevets d'invention", Paris, *Journal des Notaires et des Avocats* (1974).

[33] Cass, "Crim 29 de junio 1960", *Boletín Crim* Núm. 350 (Francia), Cass Com. 22 marzo 1971, *Boletín* IV, Núm. 84, p. 76; París 7 enero 1955, *Anales de la propiedad industrial*, 1955, 218.

[34] "SESAC X VS. Nanterre", 5 de mayo de 1981, *Expertises*, Núm. 57, Dic. 1983, p. 292, nota de Brigitte van Dousselaere en *Expertise*, núm. 18, enero 1984.

[35] Ver J. Vassagne et C. Bernard, *Resp. penal;* V. Sieber, "Infractions en matiére d'informatique", *Droit Affaires* núm. 406, sept. 1983 pt. 78 et D. Parker, *Crime by Computer ,op. cit.*

D. *La vía civil*

Fuera del contrato dos posibilidades son contemplables, según la terminología clásica: el hecho delictuoso o casi delictuoso y en una terminología moderna, el perjuicio causado a otro o el enriquecimiento provocado a otro:[36]

a) La competencia desleal

En forma sintética podemos decir que la acción de la competencia desleal es la vía jurídica que permite contrarrestar los actos de competidores que son contrarios a los usos honestos del comercio, y principalmente los que puedan crear una confusión con el establecimiento, los productos o la actividad industrial o comercial de un competidor; los alegatos falsos que tiendan a desacreditar el establecimiento, los productos, o la actividad industrial o comercial de un competidor; las indicaciones o alegatos susceptibles de inducir al público al error sobre la naturaleza, la forma de fabricación o las características de las mercancías, etcétera.

Para que un individuo (o una empresa) pueda ser objeto de una acción en competencia desleal es necesario que cause un perjuicio por el hecho de "sustraer" un secreto de empresa de manera furtiva. La acción en competencia desleal no es por tanto normalmente aplicable al encuentro de terceros, que han adquirido el secreto sin haber cometido deliberadamente un acto contrario a los usos honestos. Por regla general, se identifica esta acción en cuanto su naturaleza jurídica con la acción en responsabilidad civil prevista por la ley, como lo previene el artículo 1382 del Código Civil francés y que exigen que sean aportadas la prueba del perjuicio y la prueba de una falta cometida.[37]

Tales datos pueden ser difíciles de establecerse, aun cuando los tribunales se muestren afines a sancionar la competencia desleal. Así nos remitiremos, por ejemplo, al caso de espionaje industrial.

Hay que diferenciar esta situación de la llamada "competencia parasitaria" (normalmente no aludida en el derecho francés, pero bien conocida del derecho suizo), en la cual una empresa se aprovecha del trabajo, creatividad o reputación ajenos.[38]

---

[36] J. Carbonnier, *Droit civil*, t-II, París PUF, Colección Themis.

[37] En ese sentido ver: A Benabent, *Acción en competencia desleal*; JCI, *Competencia desleal*, fasc. IV: J. Hemaro, *Concurrence Deloyale*; Claude Lebel, *Practiques restrictives de concurrence en droit francais*, París, Libraires Techniques, 1981; *adde*. Phillipe, "Le orneau variations autour de la protection du logiciel", *Gaz. Pal.* del 6 de julio 1982.

[38] Sobre esta noción ver específicamente "La competencia parasitaria en el derecho comparado", *Actas del Coloquio de Lausana*, Ginebra, 1981.

La característica de esta acción en competencia desleal aplicada en la protección de programas, es que no puede impedir la utilización simple del programa a falta de una apropiación desleal y furtiva, lo que no excluye suponer su utilización a título supletorio de otras acciones, a efecto de sancionar no tanto la violación de un derecho privativo de propiedad incorporal (como tal oponible a todos), sino un comportamiento desleal que atente a los intereses comerciales de un competidor, particularmente en el desvío de su clientela por un riesgo de confusión presuntamente creada,[39] aun si esta función ha sido criticada como atenuación de un derecho privativo, donde no existe disposición legal o voluntad de las partes.[40]

b) El enriquecimiento sin causa

Falta hablar aún de un medio que eventualmente puede invocar aquel que, no disponiendo de medios de protección privativa, se ve desposeído de su creación por un tercero. Se trata de una acción basada en la teoría del enriquecimiento sin causa, calificado en los Estados Unidos de *injust enrichment*, y que deriva de un principio general de equidad según el cual está prohibido enriquecerse en detrimento de otro.[41]

Para triunfar en una acción basada en la teoría del enriquecimiento sin causa, el demandante debe probar que la utilización de su idea o invención por un tercero ha permitido a éste enriquecerse y que correlativamente ha provocado un empobrecimiento. Pero esas pruebas son tan difíciles de aportar en la práctica que el recurso a la teoría en cuestión es esporádicamente invocado.

Por otra parte, una regulación de tal acción (que queda aun por imaginar) no facilitaría mucho su uso, ya que podría desencadenar graves abusos, en virtud del riesgo latente de ver a particulares o empresas invocar falsamente un perjuicio (un empobrecimiento) largamente ficticio o al menos ampliamente sobrestimado.

Así, el problema de la protección de programas está lejos de ser resuelto por estas diferentes vías que podríamos calificar como clásicas, aun si las diversas instituciones jurídicas que venimos examinando ofrecen potencialmente elementos de solución importantes. Quedan aún lagunas e insuficiencias. Las dificultades de prueba podrían ser remontadas; sin embargo, quedaría por encontrar la solución adecuada.

---

[39] Nota de J. Dupichot en COM. 15 de junio 1983 (Ref. 2098) Société Produits Industriels et Metallurgiques SAPIM INOX vs. Société Cellier y otras.

[40] Roubier P., "Theorie générale de l'action en concurrence deloyale", *Rev. Trim. Droit Com.* 1948, p. 541; "Distinction entre l'action en contrefacon et l'action en concurrence deloyale", *Rev. Trim. Droit Civil* 1952, 161; *Le Droit de la Proprieté Industrielle*, t-I, Sirey, 1982 pp. 307 y sigs.

[41] Hay que reconocer la célebre fórmula de la decisión Boudier (Reg., 15 de junio 1982, D.F. 1982, 1596; S. 1983, 1281, nota LOBBE).