



El derecho a leer

Richard Stallman

*Este artículo fue publicado en el número de febrero de 1997 de **Communications of the ACM** (Vol. 40, Número 2).*

(de "El camino a Tycho", una colección de artículos sobre los antecedentes de la Revolución Lunar, publicado en Luna City en 2096)

Para Dan Halbert el camino a Tycho comenzó en la universidad, cuando Lissa Lenz le pidió prestado su ordenador. El de ella se había estropeado, y a menos que pudiese usar otro reprobaría su proyecto de fin de trimestre. No había nadie a quien se atreviera a pedirselo, excepto Dan.

Esto puso a Dan en un dilema. Tenía que ayudarle, pero si le prestaba su ordenador ella podría leer sus libros. Dejando de lado el riesgo de ir a la cárcel durante muchos años por dejar a otra persona leer sus libros, la simple idea le sorprendió al principio. Como a todo el mundo, se le había enseñado desde la escuela primaria que compartir libros era algo malo y desagradable, algo que sólo los piratas harían.

Además, no había muchas posibilidades de que la SPA (la "Software Protection Authority", o Autoridad de Protección del Software), no lo descubriese. En sus clases de programación Dan había aprendido que cada libro tenía un control de copyright que informaba de cuándo y dónde fue leído, y quién lo leía, a la oficina central de licencias (usaban esa información para descubrir piratas, pero también para vender perfiles personales a otras compañías). La próxima vez que su ordenador se conectase a la red, la oficina central de licencias lo descubriría. Él, como propietario del ordenador, recibiría el castigo más duro, por no tomar las medidas adecuadas para evitar el delito.

Lissa no necesariamente pretendería leer sus libros. Probablemente lo único que ella necesitaba era escribir su proyecto. Pero Dan sabía que ella provenía de una familia de clase media que a duras penas se podía permitir pagar la matrícula, sin pensar en las tasas de lectura. Leer sus libros podía ser la su única forma de terminar la carrera. Entendía la situación; él mismo había pedido un préstamo para pagar por los artículos de investigación que leía (el 10% de ese dinero iba a parar a los autores de los artículos, y como Dan pretendía hacer carrera en la universidad, esperaba que sus artículos de

investigación, en caso de ser citados frecuentemente, le dieran los suficientes beneficios como para pagar el crédito).

Más tarde, Dan descubrió que hubo un tiempo en el que todo el mundo podía ir a una biblioteca y leer artículos, incluso libros, sin tener que pagar. Había investigadores que podían leer miles de páginas sin necesidad de becas de biblioteca. Pero desde los años 90 del siglo anterior, tanto las editoriales comerciales, como las no comerciales, habían empezado a cobrar por el acceso a los artículos. En el 2047, las bibliotecas de acceso público eran sólo un vago recuerdo.

Había formas de evitar los controles de la SPA y la oficina central de licencias, pero también eran ilegales. Dan había tenido un compañero de su clase de programación, Frank Martucci, que consiguió un depurador ilegal, y lo usaba para evitar el control de copyright de los libros. Pero se lo contó a demasiados amigos, y uno de ellos lo denunció a la SPA a cambio de una recompensa (era fácil tentar, para traicionar a sus amigos, a estudiantes con grandes deudas). En 2047 Frank estaba en la cárcel; pero no por pirateo, sino por tener un depurador.

Dan supo más tarde que hubo un tiempo en el que cualquiera podía tener un depurador. Incluso había depuradores libremente disponibles en la red. Pero los usuarios normales empezaron a usarlos para saltarse los controles de copyright, y finalmente un juez dictaminó que ese se había convertido en su uso práctico. Eso quería decir que los depuradores eran ilegales y los programadores que los habían escrito fueron a parar a la cárcel.

Obviamente, los programadores necesitan depuradores, pero en el 2047 sólo había copias numeradas de los depuradores comerciales, y sólo disponibles para programadores oficialmente autorizados. El depurador que Dan había usado en sus clases de programación estaba detrás de un cortafuegos para que sólo se pudiese utilizar en los ejercicios de clase.

También se podía saltar el control de copyright instalando un núcleo del sistema modificado. Dan llegó a saber que hacia el cambio de siglo había habido núcleos libres, incluso sistemas operativos completos. Pero ahora no sólo eran ilegales, como los depuradores: no se podía instalar sin saber la clave de root del ordenador, cosa que ni el FBI ni el servicio técnico de Microsoft te darían.

Dan llegó a la conclusión de que simplemente no podía dejarle su ordenador a Lissa. Pero no podía negarse a ayudarle, porque estaba enamorado de ella. Cada oportunidad de hablar con ella era algo maravilloso. Y el hecho de que ella le hubiese pedido ayuda podría significar que sentía lo mismo por él.

Dan resolvió el dilema haciendo algo incluso más increíble, le dejó el ordenador, y le dijo su clave. De esta forma, si Lissa leía sus libros, la oficina central de licencias pensaría que quien estaba leyendo era él. Seguía siendo un delito, pero la SPA no lo detectaría automáticamente. Sólo podrían saberlo si Lissa lo denunciaba.

Si la universidad descubriese que le había dado su clave a Lissa significaría la expulsión para los dos, independientemente de para qué hubiese usado ella la clave. La política de la universidad era que cualquier interferencia con sus métodos de control sobre el uso de los ordenadores era motivo para una acción disciplinaria. No importaba si se hubiera hecho o no algún daño, el delito era el hecho de dificultar el control. Se asumía que esto significaba que se estaba haciendo algo prohibido, y no necesitaban saber qué.

En general los estudiantes no eran expulsados por eso -no directamente-. En su lugar se les prohibía el acceso a los ordenadores de la universidad, lo que inevitablemente significaría reprobar todas sus asignaturas.

Dan supo más tarde que ese tipo de políticas en la universidad empezaron en la década de 1980, cuando los estudiantes comenzaron a usar ordenadores masivamente. Antes de eso, las universidades tenían una actitud diferente: sólo se penalizaban las actividades dañinas, no las que eran meramente sospechosas.

Lissa no denunció a Dan a la SPA. Su decisión de ayudarlo llevó a que se casasen, y también a que cuestionasen lo que les habían enseñado cuando eran niños sobre el pirateo. Empezaron a leer sobre la historia del copyright, sobre la Unión Soviética y sus restricciones sobre las copias, e incluso sobre la constitución original de los Estados Unidos. Se mudaron a Luna, donde se encontraron con otros que de la misma forma intentaban librarse del largo brazo de la SPA. Cuando empezó el Levantamiento de Tycho en 2062, el derecho universal a leer se convirtió en uno de sus objetivos fundamentales.

Nota del autor

Esta nota fue actualizada en 2002

El derecho a leer es una batalla que se está librando hoy en día. Nuestra forma de vida actual podría tardar 50 años en desvanecerse, pero muchas de las leyes y prácticas descritas más arriba ya han sido propuestas, o por la administración Clinton o por las editoriales.

Hasta hace poco había una excepción: la idea de que el FBI y Microsoft se guardaran las claves de root de los ordenadores personales, y no dejaran obtenerlas a los usuarios no fue propuesta hasta 2002. A esto se le llamó "computación confiable" o "palladium".

En 2001, el senador Hollings, apoyado financieramente por la Disney, propuso un proyecto de ley, llamado SSSCA, que requeriría que cada ordenador nuevo tuviera restricciones para efectuar copias, que los usuarios no podrían evitar. En la misma línea que la del chip Clipper y otras propuestas similares del gobierno de los EE.UU. sobre custodia de claves de encriptación, esta es una tendencia a largo plazo: los sistemas de ordenadores se configuran cada vez más para dar control sobre el ordenador a terceras partes en lugar de a las personas que realmente lo utilizan. La SSSCA ha sido llamada desde entonces

la CBDTPA (denotando "Consume But Don't Try Programming Act", "Consume Pero Ni Intentas Programar").

En 2001 los EE.UU. comenzaron a intentar el uso del propuesto Tratado del Área de Libre Comercio de las Américas (ALCA) para imponer las mismas reglas en todos los países del hemisferio occidental. El ALCA es uno de los tratados llamados "de libre comercio" realmente diseñados para darles a las empresas mayor poder frente a los gobiernos democráticos; imponer leyes tales como la DCMA es típico de este espíritu. La Electronic Frontier Foundation le solicita a las personas que expliquen a esos gobiernos por qué deberían oponerse a tales planes.

La SPA, que realmente significa "Software Publisher's Association" (Asociación de Editores de Software), ha sido reemplazada en este rol policíaco por la BSA, o "Business Software Alliance". Esta no es una fuerza policíaca, pero extraoficialmente actúa como si lo fuera. Utilizando métodos que recuerdan a la antigua Unión Soviética, invita a la gente a informar a sus compañeros de trabajo y amigos. En 2001 una campaña de terror de la BSA en Argentina realizó amenazas veladas de que aquellos que compartieran programas de ordenador terminarían siendo violados en prisión.

Cuando se escribió esta historia, La SPA estaba amenazando a pequeños proveedores de Internet (ISP) para que les permita controlar a sus usuarios. La mayoría de ellos cedieron al ser amenazados, ya que no podían costearse la pelea judicial en los tribunales (Atlanta Journal-Constitution, 1 Oct 96, D3). Al menos un ISP, "Community ConneXion" en Oakland CA, se negó a aceptar las presiones, y fue eventualmente demandado. La SPA luego retiró la demanda, pero obtuvo la DMCA ("Digital Millenium Copyright Act", o Ley del Copyright del Milenio Digital), la cual les dio el tipo de poder que buscaban.

Las políticas de seguridad descritas arriba no son imaginarias. Por ejemplo, un ordenador de una universidad del área de Chicago muestra el siguiente mensaje al conectarse al sistema (las comillas están en el original):

"Este sistema sólo puede ser utilizado por usuarios autorizados. Cualquier individuo que use esta sistema sin autorización, o excediendo su autorización está sujeto a ser monitorizado por el personal del sistema. Al controlar usuarios realizando actividades no autorizadas o durante el mantenimiento del sistema, las actividades de usuarios autorizados pueden ser monitorizadas. Cualquiera que use este sistema acepta expresamente tal monitorización y queda advertido de que si ese control revela posibles indicios de actividades ilegales o violación de las normas de la Universidad, el personal de mantenimiento del sistema puede proporcionar esas evidencias a las autoridades de la Universidad o a las fuerzas de seguridad".

Esta es una aproximación interesante a la Cuarta Enmienda: forzar a los usuarios a declinar por adelantado los derechos en ella contemplados.

Referencias

- El Libro Blanco de la Administración: "Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights", (1995).
- "An explanation of the White Paper: The Copyright Grab", Pamela Samuelson, Wired, Jan. 1996
- "Sold Out", James Boyle, New York Times, 31 March 1996
- "Public Data or Private Data", Washington Post, 4 de noviembre de 1996. Teníamos un enlace a esta referencia, pero el Washington Post decidió comenzar a cobrar a los usuarios que quisieran leer artículos en su página web, y por lo tanto hemos decidido borrar el enlace.
- "Union for the Public Domain", una organización que pretende resistir y revertir la sobreextensión de los poderes de la propiedad intelectual y patentes.

Este ensayo ha sido publicado en "Free Software, Free Society: The Selected Essays of Richard M. Stallman".