

De Automatas y Cimarrones: una reseña sobre “La Ética del Hacker y el Espíritu de la Información” de Pekka Himanen

David A. Hernández Aponte

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres – CENDITEL
Mérida, Venezuela
dhernandez@cenditel.gob.ve

Fecha de recepción: 28/10/2016

Fecha de aceptación: 02/11/2016

Pág: 203 – 209

Resumen

Este texto pretende analizar, de manera sencilla, la obra de Himanen, y se aprovecha para traer a colación situaciones que sucedieron en poco más de 10 años luego que se publicó el libro, de esta manera comparar cuánto ha cambiado, si es que lo ha hecho, la tecnología e incluso la percepción de la ética hacker en estos últimos años.

La ética hacker y el espíritu de la era de la información es un libro escrito por Pekka Himanen con prólogo de Linus Torvald y epílogo de Manuel Castells, publicado en 2002. En esta obra se da un análisis exhaustivo de la ética hacker, el libro se divide principalmente en tres capítulos, cada uno dedicado, según la percepción del autor, a un nivel de la ética hacker, estos son, la ética del trabajo, la ética del dinero y la ética de red.

Palabras Clave: himanen, hacker, cracker, ética

(H|Cr)ackers

Antes que todo, digamos que un *hacker informático* lo podemos entender como aquella persona que, entre muchas otras cosas, se divierte programando, desarrollando, innovando, estudiando, entendiendo sistemas, etc., que además es bueno en estas áreas y cuyas habilidades no las usa en la búsqueda del perjuicio a otros, asimismo, está en su filosofía enseñar sus creaciones y compartir sus conocimientos. En los últimos años se ha venido confundiendo, en algunos casos quizás de manera inocente y en otros con toda intención¹, a los hackers con

¹El caso mas sonado en los últimos años de criminalización del término es el protagonizado por la Real Academia Española (RAE) en 2014, cuando en su edición 23ª iguala al hacker con el pirata informático. Ver: <http://www.genbeta.com/actualidad/la-rae-criminaliza-a-los-hackers-igualando-su-definicion-a-la-de-los-piratas-informaticos>

criminales informáticos, mal llamados piratas cibernéticos, personas que se encargan de hacer daño a través de las redes, a estos criminales, en el mundo informático se les denomina *crackers*.

Ahora hagamos un ejercicio y extrapolemos el término hacker más allá de la actividad informática. El hacker no necesariamente se refiere al mundo computacional, el hacker también puede estar ubicado en cualquier otra área practicada por los seres humanos, por ejemplo, un fotógrafo puede ser un hacker de la exposición de la luz y de la composición, un carpintero puede ser un hacker de la madera; y así, podemos aplicar el término a cualquier otra actividad. Si vemos sus desempeños como arte y como artesanos, estas personas son innovadores, manejan plenamente las herramientas, son curiosos, virtuosos, excelsos y mucho más; estas personas son hackers.

Ley de Linus

Deseaba dar una breve y simple definición de hackers dado que el prólogo del libro nos introduce con lo que Linus Torvald humildemente llamó la “Ley de Linus”, la cual según él, explica porqué el hacker es como es. Aquí nos dice que todas nuestras motivaciones como seres humanos se agrupan en tres categorías, pero lo más importante en todo esto es que el progreso debe pasar por cada una de estas categorías en un cierto orden, las categorías y su orden de transición son: *sobrevivencia*, *vida social* y *entretenimiento*. La sobrevivencia se explica por sí sola, la capacidad de un individuo para mantenerse con vida. La vida social sería la razón por la que el individuo arriesgaría la vida y esto se da por los vínculos sociales que tengamos con un elemento, llámese familia, pareja, patria, etc. Por último tenemos el entretenimiento como factor para, como diríamos coloquialmente, ponerle sabor a la vida.

La relación de la Ley de Linus con los hackers lo explica justamente con los desarrolladores del núcleo Linux: el entretenimiento como nirvana. Entretenimiento en el sentido de hacer cosas interesantes y que van más allá de hacer estas cosas interesantes como un simple medio para poder obtener el alimento para su sobrevivencia y logros en su vida social.

La ética hacker del trabajo

Para describir la primera parte del libro, *la ética hacker del trabajo*, Himanen señala como para los hackers el uso del computador significa diversión, entretenimiento, un goce a la hora de programar, un juego. Me atrevo a decir que, a todos los que nos gusta programar, nos pasa que cuando empezamos a codificar cuesta trabajo que nos detengan, nos entusiasamos a tal punto que pasamos horas escribiendo código, resolviendo errores y viendo como evoluciona nuestro programa para que termine haciendo lo que queremos que haga. Este sentido lúdico del trabajo en el hacker informático es tomado como referencia por Himanen para definir la ética hacker del trabajo, en contraste con la *ética protestante del trabajo*, donde el fin único de cada individuo es el trabajo. Acá se establecen semejanzas donde la ética hacker del trabajo se acerca a la academia, a la antigua academia, entendiéndose como las viejas escuelas griegas donde el maestro no imponía las ideas sobre un grupo de sumisos receptores sino que era un guía para

la búsqueda de una verdad en colectivo. Por otro lado, a la ética protestante del trabajo la equipara con los monasterios, donde los monjes viven para el trabajo y donde además no se les tiene permitido el cuestionamiento de las órdenes o tareas impuestas, siempre obedeciendo las directrices de un superior, un comportamiento, por demás, digno de ser reproducido. El autor nos ejemplifica brevemente como la iglesia protestante influyó para cambiar los dogmas sobre el trabajo en contraposición a la postura de la iglesia preprotestante, mientras que la ética protestante del trabajo se centra en el trabajo como objetivo de vida, la ética preprotestante del trabajo tiene como meta el descanso.

Algo que me resulta ocurrente por parte del autor es la asociación de las diferentes éticas de trabajo con algunos días de la semana. La ética protestante es relacionada con el viernes, que a su vez es asociado con el trabajo, mientras que la ética preprotestantes es vinculada con el domingo que significa descanso y goce. Así, mientras que para los unos el propósito de la vida era el viernes, para los otros el propósito de la vida era el domingo. La ética hacker del trabajo la acerca más al domingo que al viernes. En lo personal, yo hubiese preferido asociar la ética protestante con los lunes, el primer día de trabajo posterior al descanso, y a la ética hacker del trabajo con el sábado, un día libre en el que a veces usamos algunas horas para afinar, terminar o adelantar tareas de la semana, donde el entretenimiento y el descanso conviven armónicamente sin turnos preestablecidos.

El tiempo y la creatividad en lo laboral

En el libro también se nos ilustra un poco la relación que tiene el hacker con el tiempo, y la forma como hace uso de éste a la hora de trabajar. Mucho se escucha como hoy en día algunas empresas dan ciertas flexibilidades en el tema horario laboral, lo hacen para propiciar la creatividad de los trabajadores, las empresas se apoyan en la confianza depositada en sus trabajadores para el cumplimiento de los objetivos asignados. Estas empresas entienden que el hacker no es el típico ser acostumbrado a cumplir un horario fijo donde se trabaja ocho horas diarias —o más— pegado al computador. El hacker es un ser que cumplirá con su meta, a su ritmo, y esto no quiere decir que tardará más que un empleado tradicional, de hecho, esta *libertad* le permite cumplir con su trabajo satisfactoriamente.

En un sentido más amplio, el capítulo habla de como el hacker puede liberarse un poco de esa atadura del trabajo, si bien no lo descuidaba, no tenía problemas para dedicar tiempo a otras actividades no relacionados con el ámbito laboral, algo que difícilmente se logra en la ética protestante del trabajo, allí donde se vive en un viernes eterno. En el capítulo también se dedica gran parte a hablar de la optimización, como se ve la optimización desde el punto de vista de la ética hacker del trabajo y desde la ética protestante del trabajo, en la primera el uso del tiempo, los hábitos de trabajo son autorregulados por la persona, se habla de un “tiempo flexible”, mientras que en la segunda se pierde esta autorregulación y se es prisionero de los horarios laborales establecidos en la sociedad actual.

Las tecnologías avanzan pero el modelo de trabajador como autómatas aún se mantiene con firmeza, cambiar el paradigma de contrato de personal midiéndose en horas de trabajo

en lugar de hacerlo por cumplimiento de metas es aún escaso, hemos sustituido el látigo que hostiga al esclavo por herramientas electrónicas, como aplicaciones que capturan la pantalla del computador cada tantos segundos y envían estas capturas al empleador, detección de movimiento de ratón, detección de entrada por teclado, cámaras, etc. Al no percibir cambios en un tiempo determinado se descuenta la hora de trabajo. Apartarse del computador para ir al baño, ir a la cocina a preparar y tomar un café, hacer anotaciones, investigar, despejar la mente para resolver un problema, son situaciones bastante limitadas en estas modalidades de trabajo.

El dinero no lo es todo

El tema del dinero también es analizado en la obra, Himanen continúa contrastando la ética protestante con la ética hacker, de las motivaciones capitalistas y filosóficas que mueven a las personas.

En este apartado, me gustaría recordar a Aaron Swartz. Swartz fue un notable programador, en 2007 presentó durante la Conferencia de Computación Tathva en Calcuta una charla con el nombre "Cómo conseguir un trabajo como el mio", durante parte de la charla nos relataba la experiencia que vivió durante la venta de la página web Reddit. Me parece que ilustra un poco como es la relación entre los hackers, el dinero y el trabajo o entretenimiento. Nos decía Swartz[1]:

Negociamos durante meses. Primero, discutimos acerca del precio. Preparamos planes y hojas de cálculo y fuimos a la sede principal para hacer la presentación, y tener reuniones y llamadas telefónicas interminables. Finalmente ellos rechazaron nuestra oferta, y nos retiramos. Luego ellos cambiaron el tono, finalmente estrechamos nuestras manos y cerramos el trato, pero sólo para volver a comenzar las negociaciones en algún otro punto clave, y solamente para retirarnos nuevamente. Tuvimos que retirarnos tres o cuatro veces antes de finalmente tener un contrato en el cual estuviéramos de acuerdo. Dejamos de hacer trabajo real por seis meses.

Comencé a volverme loco por tener que pensar tanto acerca del dinero. Empezamos a ponernos susceptibles a causa del estrés y por la falta de productividad en el trabajo. Comenzamos a gritarnos entre nosotros mismos, nos dejamos de hablar para luego lanzar renovados esfuerzos para trabajar juntos, solamente para comenzar a gritarnos de nuevo. La compañía casi se cae a pedazos antes que el acuerdo se concretara.

Pero eventualmente fuimos a las oficinas de nuestros abogados para firmar todos los documentos y a la mañana siguiente el dinero estaba en nuestras cuentas bancarias. Estaba hecho.

Todos volamos a San Francisco y comenzó el trabajo en las oficinas de Wired News (fuimos adquiridos por Condé Nast, una gran compañía editorial la cual era dueña de Wired, junto a algunas otras revistas).

Me sentía miserable. No podía soportar a San Francisco. No podía aguantar la vida de oficina. No podía soportar a Wired. Me tomé unas largas vacaciones de navidad. Me enfermé. Pensé en el suicidio. Huí de la policía. Y cuando regresé en la mañana del lunes, se me solicitó la renuncia.²

Este capítulo en la historia de Swartz refleja como grandes cambios pueden afectar a una persona, mi intención es mostrar que durante meses Swartz dejó de hacer lo que le gusta hasta el punto de hacerlo sentir miserable, a pesar de las grandes cantidades de dinero. En un breve periodo de tiempo Swartz pasó de ser un hacker informático a un empresario para luego hacer el papel de empleado, y finalmente ser un desempleado.

Aaron Swartz lamentablemente se suicidó el 11 de enero de 2013, tenía sólo 26 años de edad, en el 2011 fue acusado de fraude informático y obtención ilegal de documentos al descargar publicaciones académicas de la biblioteca digital JSTOR a través de la red del Instituto de Tecnología de Massachusetts (MIT). Tanto JSTOR como MIT retiraron la denuncia pero el gobierno estadounidense prosiguió con la acusación, Swartz enfrentaba pena de 35 años de cárcel y una multa de un millón de dólares.

Swartz fue un programador y activista informático, un hacker. A los 14 años de edad fue coautor de las especificaciones RSS 1.0, también fue cofundador de la página Reddit, codiseñador del formato Markdown, creador de la arquitectura del sistema Open Library, fundador de Demand Progress, una organización para la lucha en contra de la censura en internet, con Demand Progress ayudó a movilizar activistas para frenar los proyectos de censura de la internet SOPA/PIPA, colaboró en el primer borrador de la licencia Creative Commons.

No para todos el dinero es el fin último, para unos cuantos lo es el libre acceso al conocimiento, en su forma más amplia, entendiéndose no sólo el acceso a éste sino también su difusión. No digo que el dinero no sea necesario, es una necesidad que hemos creado y mantenido, le hemos asignado esa importancia artificial porque es el método de canje preferido en la sociedad moderna. Me refiero a que hay una diferencia entre vivir para ser un acumulador de capital o vivir para poder satisfacer nuestras sanas pasiones.

Nética

La última parte del libro toca el punto de la ética de red, llamada también nética y que es definida por Himanen^[2] como “la relación que el hacker mantiene con las redes de nuestra actual sociedad red” (p.66). Aquí se relata un poco la historia de varios pioneros en la lucha contra la censura en internet como Mitch Kapor, John Perry Barlow, John Gilmore y grupos como la Electronic Frontier Foundation (EFF), XS4ALL y Witness, que incluso jugaron papeles importantes en guerras como la de Kosovo.

En nuestros días una de las organizaciones que se dedica a publicar documentos filtrados y considerados sensibles por el gobierno estadounidense es WikiLeaks, en 2007 gana notoriedad a nivel mundial al publicar un video donde soldados estadounidenses asesinan desde un helicóptero

²Traducción propia.

a un grupo de civiles en la ciudad de Bagdad, entre los asesinados se encontraba un reportero de Reuters y su ayudante. La analista de inteligencia Chelsea Manning fue condenada en 2013³ a cumplir condena de 35 años por estas filtraciones. En los años subsiguientes la página ha seguido revelando información de indignantes actividades estadounidenses en territorios invadidos por este país. Su fundador Julian Assange se encuentra actualmente asilado en la embajada ecuatoriana de Londres, ya que tiene orden de extradición por supuestos delitos sexuales en Suecia.

El tema de la seguridad y vigilancia en internet también es tratado en este capítulo, si bien se hace mención de las acciones de algunos gobiernos para poder controlar lo que sus habitantes pueden visitar, el panorama ha cambiado desde el 2002, a medida que la el acceso a internet se expande, es mayor la posibilidad de mantener vigilado a los usuarios, el mayor caso de vigilancia gubernamental hasta la fecha es el revelado por Edward Snowden, consultor tecnológico estadounidense, ex empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA). En 2013⁴ Snowden hace público a través de los periódicos The Guardian y The Washington Post una serie de documentos clasificados donde se revela una red de vigilancia gubernamental liderada por la NSA. Las técnicas utilizadas para la captura ilegal de datos por parte de agencias estatales abarca el uso de sistemas especializados de vigilancia como PRISM y XKeyscore entre otros, hasta el uso de “puertas traseras” (brechas de seguridad intencionales) en programas de computadora y sistemas operativos privativos, incluyendo sistemas operativos para teléfonos móviles.

También es importante destacar que en muchos casos no es necesario el uso de sistemas espías especializados en la captura de datos para la obtención de información privada. Con el auge de los sistemas de red social, hoy en día les entregamos a las empresas y gobiernos, sin coacción alguna, nuestros datos, publicamos libremente nuestras ubicaciones, lo que compramos, lo que comemos, lo que nos gusta y lo que no, lo que estamos haciendo, lo que estamos pensando; en resumen, lo que somos.

Conclusiones

Himanen se apoya en la Ley de Linus para el desarrollo del libro, tomando como cimiento las motivaciones del hacker procede a elaborar las diferentes éticas que desde su mirada componen al hacker. La pasión o goce sería la motivación última y principal que estimula al hacker, el reconocimiento de los pares por las creaciones expuestas forma parte del tejido social que se quiere exponer en la fase de vida social, a este estado yo le llamaría *ego*, en un buen sentido si se me permite, que en ocasiones choca con la poca modestia que caracteriza a muchos hackers.

Además, el escritor explota todo el significado que encierra la ética protestante y la

³Bradley Manning, condenado a 35 años de cárcel por las filtraciones a Wikileaks. Ver: <http://www.xataka.com/privacidad/bradley-manning-condenado-a-35-anos-de-carcel-por-las-filtraciones-a-wikileaks>

⁴Cronología de las revelaciones de Edward Snowden. Ver: <http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html>

aprovecha como referencia principal para sentar una base comparativa entre las diferentes visiones expuestas.

Scientia potentia est —el conocimiento es poder—, frase más que pertinente en el tema que nos reúne. El capitalismo es un sistema antagónico con la filosofía hacker, el capitalismo es el sistema que hace uso de la explotación de recursos con el objetivo de acumular la mayor cantidad de riqueza y poder, sin importar los medios. Mientras el capitalismo se adapta y busca hacerse de herramientas que le permitan controlar el poder, entre las que se encuentra el conocimiento, el hacker busca que el conocimiento esté al alcance de todos pues su objetivo de vida dista del capital. Pero como la filosofía hacker va en contra de estos intereses, muchas veces esa búsqueda termina en persecución, por nombrar la situación menos agravante.

El software libre está intrínsecamente relacionado con la filosofía hacker, de hecho la filosofía del software libre y la del código abierto nacen de los hackers, la libertad del conocimiento, el libre acceso a éste, están arraigados en el hacker, antes de 1970, en la informática, era la filosofía que imperaba, era algo natural, no tenía nombre ni estaba definida como lo está ahora en nuestros días, era la práctica cotidiana. La computación ha evolucionado gracias a esos avances libres. Sin el conocimiento libre no existirían las teorías científicas que impulsaron los avances de la humanidad.

Me pregunto y dejo para la reflexión: ¿Qué pasaría si el mundo dejara de funcionar bajo el modelo actual, imperantemente capitalista, esencialmente individualista, donde las personas no se preocupan por nadie salvo por sí mismas y por el dinero que puedan acumular? ¿Podemos imaginar un mundo libre de patentes donde el conocimiento se encuentre al alcance de todos sin restricciones? ¿Podemos soñar con un modelo que apunte más a la ética hacker, que apunte al sábado?

Bibliografía

- [1] Swartz, A. (2007). *How to Get a Job Like Mine*. Recuperado el 25 de octubre de 2016 desde <http://aaronsw.jottit.com/howtoget>
- [2] Himanen, P. (2002). *La ética del Hacker y el espíritu de la era de la información*. Barcelona: Destino