Criminalidad de cuello blanco

Una nueva visión del concepto

Un trabajo de Carlota Barrios Vallejo

www.crimiperito.es

2014

ÍNDICE

Introducción Página 2

Otras formas de crimen de cuello blanco Página 5

El hacking Página 5

La ciencia Página 10

Las multinacionales Página 13

Conclusiones Página 17

Bibliografía Página 20

Introducción.

A menudo, el término delincuente de cuello blanco, inspira en los no entendidos en el tema un sentimiento algo poético.
Cuando aún estaba lejos de ser estudiante de Criminología, solía idealizar a los delincuentes de ese tipo imaginando a importantes ejecutivos que robaban diamantes con zapatos italianos brillantes y corbatas de seda.
Los medios de comunicación, las novelas de misterio y el cine, han contribuido a que nos formemos una imagen poco real e incluso ridículamente idealizada, de este tipo de criminales.

Lo cierto es que este tipo de criminalidad existe desde hace mucho tiempo, pues desde los comienzos de la historia, siempre han existido personas poderosas que se han aprovechado de su situación para delinquir.

Sin embargo, los comienzos del interés por lo que hoy conocemos como criminalidad de cuello blanco, se sitúan en el año 1940, cuando un sociólogo llamado Edwin H. Sutherland acuñó el término de *crimen de cuello blanco* (white collar crime). [1]

Desde entonces, la criminalidad de cuello blanco es conocida en todo el mundo y se ha convertido en un tema de gran interés para los Criminólogos. En la segunda mitad del siglo XX, son muchos los autores que se han aventurado a modificar o ampliar la definición que Sutherland propuso, pero incluso a día de hoy, el concepto de criminalidad de cuello blanco sigue sin estar claro y hay multitud de definiciones según el país, el campo de estudio e incluso la época en la que nos encontremos.

Este trabajo pretende revisar las definiciones de criminalidad de cuello blanco más interesantes desde el punto de vista criminológico, con el fin de proponer un nuevo concepto que atienda sobretodo a la multidisciplinaridad que caracteriza a la Criminología como ciencia social.

[1] Agustín Fernández Albor, "Estudios de criminalidad económica" – Editorial Bosch, 1978 Barcelona – Pág. 10

Para empezar, el concepto social de cuello blanco (white collar) lo acuñó Pulitzer Prize en 1930 y viene de la época en la que los jefes y altos ejecutivos de las empresas vestían con camisa blanca, así como sus empleados con camisa azul (blue collar). Con el tiempo, este término se fusionó con la criminalidad, haciendo referencia a aquellos altos mandos, directivos, etc., que delinquían para conseguir mayores beneficios económicos.

Al final, Sutherland le otorgó a este tipo de delitos el nombre de "white collar crime" (crimen de cuello blanco) y definió, desde el punto de vista sociológico, al delincuente que lo practicaba como "*una persona de nivel económico elevado que viola las reglas legales (o no) destinadas a fijar sus actividades profesionales*".

El término de criminalidad de cuello blanco, se conoce en otros idiomas como 'white collar criminality', 'weisse-kragen kriminalität', 'criminalité en col blanc', 'criminalité en collet blanc', 'criminalità in colleti bianchi' o 'in guanti gialli'. En español, también se conoce como criminalidad de guante blanco, aunque este término no es del todo correcto y hoy en día se utiliza menos frecuentemente.

Ahora bien, si Sutherland relaciona los delitos de cuello blanco con personas de nivel económico alto, ¿con qué lo relacionan otros autores?

Middendorff, por ejemplo, compara el crimen de cuello blanco con el fraude fiscal, mientras que Hartung lo limita al marco de las actividades de establecimientos comerciales.

El autor Agustín Fernández Albor propone un interesante punto de vista respecto al crimen de cuello blanco añadiendo que, "*estos dos últimos autores, que identifican el crimen de cuello blanco con el crimen económico, parten de un malentendido que tiene origen en las obras de Sutherland, que bajo el concepto de 'white collar crime' había descrito sobretodo las violaciones económicas y había descuidado las contravenciones de otras personas respetables, como por ejemplo los hombres de ciencia*" [2]

Lo que trato de destacar en la cita de Fernández Albor, es concretamente la frase "*había descuidado las contravenciones de otras personas respetables*", porque ahí es,

[2] Agustín Fernández Albor, "Estudios de criminalidad económica" – Editorial Bosch, 1978 Barcelona – Pág. 20

precisamente, donde quiero centrar la atención a la hora de estudiar las nuevas formas de delincuencia de cuello blanco.

Dado que nos interesa conectar el término crímenes de cuello blanco con referencias que no atiendan sólo al nivel económico del delincuente, resulta muy adecuado el punto de vista de Courakis, que entiende que debe existir una relación con su actividad profesional.
Al mismo tiempo, Clinard añade que no es el nivel socioeconómico el que juega un papel importante en la concepción del delito de cuello blanco, sino más bien su actividad profesional. [3]

En estos momentos, resulta de crucial importancia entender que no todos los delincuentes de cuello blanco tienen por qué gozar de un estatus elevado gracias a su nivel económico, sino que también pueden hacerlo mediante el desempeño de una carrera profesional.
A lo largo de este trabajo, centraremos nuestra atención en aquellas personas, que, por no tener un nivel económico especialmente llamativo, han sido tachadas de la lista de posibles criminales de cuello blanco, pero que sin embargo, cuentan con un historial aparentemente impecable, una buena reputación y una condición social que les permite acceder, por ejemplo, a información valiosa.

Algunas de las características comunes a los delitos de cuello blanco que trataremos a continuación son:

- Forma ingeniosa de su ejecución.
- Estimar que se trata de simples y autorizadas relaciones comerciales ilegales pero no criminales.
- Requieren conocimientos técnicos especiales.[4]

[3] Agustín Fernández Albor, "Estudios de criminalidad económica" – Editorial Bosch, 1978 Barcelona – Pág. 20
[4] Agustín Fernández Albor, "Estudios de criminalidad económica" – Editorial Bosch, 1978 Barcelona – Pág. 18

Otras formas de crimen de cuello blanco.
El hacking.

Paul Baram es para muchos el hacker más famoso de la historia y fue la persona que acuñó el término de *hacker*, que podemos definir como aquella persona que accede a máquinas ajenas sólo por el reto que supone y la curiosidad de saber si lo conseguirá o no, si será mejor que el administrador que gestiona esa máquina o red, aprendiendo de esta manera cada vez más y más cosas acerca de lo que realmente le interesa: La informática. [5]
El término hacker, por motivos mediáticos, se ha confundido con hacker malicioso, intruso o asaltante mal intencionado.

Al mismo tiempo, Eric S. Raymond es considerado una personalidad relevante en la historia de la informática, especialmente en el mundo del software libre, y define a los hackers de varias formas en su popular *Jargon File*:

1. Alguien que disfruta explorando los sistemas y programas y sabe cómo sacarles el máximo provecho, al contrario que la mayoría de los usuarios que prefieren conocer sólo lo imprescindible.
2. Entusiasta de la programación (a veces de forma obsesiva).
3. Alguien que aprecia el valor de hackear.
4. Persona que es buena programando de forma rápida.
5. Experto en un programa concreto o especialmente hábil en el manejo de un programa o sistema determinado.
6. Experto o entusiasta de cualquier clase.
7. Alguien que disfruta con el desafío intelectual de superar las dificultades de forma creativa.
8. Mala persona que trata de descubrir información secreta. En este caso debe utilizarse el término *cracker*.

Raymond puntualiza que las definiciones 1 a 5 comprenden un grupo de gente que se une para compartir sus habilidades.

[5] Carlos Míguez Pérez, Justo Pérez Agudín y Abel Mariano-Matas García, "La Biblia del Hacker" – Editorial Anaya, 2003 Madrid – Pág. 27

Por otro lado, los autores Carlos Míguez Pérez, Justo Pérez Agudín y Abel Mariano-Matas García, nos ofrecen una clara clasificación de los tipos de intrusos, que nos puede ayudar a entender lo que realmente supone ser un hacker:

- Cracker: En realidad son hacker, pero sus intenciones tienen un fin ilícito, de lucro personal o venganza. Quieren demostrar de lo que son capaces de hacer, pero han dejado de lado la verdadera filosofía del hacker.

- Phreaker: Son cracker de las redes de telefonía y comunicaciones. A veces cuentan con conocimientos de telefonía adquiridos de dichas compañías. El phreakin consiste en los diferentes procedimientos utilizados por determinadas personas, las cuales, mediante el uso del hardware o software, logran engañar a las empresas de telecomunicaciones utilizando sus servicios sin pagar.

- Lammer: Son novatos que desean llegar a ser hacker y se denominan como tal sin serlo. Son personas que se aprovechan de todas las herramientas y programas que circulan por la red, poniéndolos en funcionamiento sin entender cómo funcionan y en qué se basan los conocimientos de fondo utilizados en su desarrollo. Sus acciones van encaminadas a molestar o a ganar notoriedad dentro de su círculo de amigos. Los verdaderos hacker muestran mucha repulsa hacia este tipo de individuos.

- Copyhackers: Son individuos que roban conocimientos de los hacker, sus herramientas y programas, para después suplantarlos y poder comercializarlos.

- Newbie: Son aspirantes a hacker, que han entendido la verdadera filosofía del hacking; su intención es ir aprendiendo y superando retos, con el fin de llegar a lo más alto en el conocimiento de la informática y de los ordenadores.

- Wannaber: Es aquel individuo que como gran sueño, aspira a ser un hacker, pero cuyas capacidades intelectuales están muy por debajo del nivel necesario para llegar a los conocimientos requeridos para ello.

- Samurai: Son los verdaderos mercenarios de la red; no les interesa la colectividad, van por libre y están dispuestos a reventar cualquier sistema si hay algo que les interesa para su lucro o hay alguien dispuesto a pagar por su trabajo.

- Pirata informático: Este término se utiliza incorrectamente como sinónimo de hacker. Son los más peligrosos desde el punto de vista de los derechos de autor, pues hacen copias de todo tipo de programas comerciales, como DVDs o CD-ROMs musicales, que pueden incluirse en soportes digitales y los venderse ilegalmente.

- Programadores de virus informáticos: Son personas con amplios conocimientos de programación, sistemas y redes. Inicialmente sus creaciones son meros desafíos, pero cuando éstas salen de sus "laboratorios" por el motivo que sea, causan muchos dolores de cabeza a empresas y usuarios. Esto ha provocado que en los últimos años proliferen las empresas que crean antivirus.

- Ciberterroristas: Son expertos en informática y hacking que ponen sus conocimientos al servicio de países, organizaciones o causas que persiguen el espionaje o el sabotaje informático de otros, a los cuales consideran sus enemigos. [6]

Por lo tanto, la mala fama que persigue a los hacker, no siempre se corresponde verdaderamente con sus actividades, sino que más bien se trata de una serie de errores de terminología. Cuando nos referimos a los hacker como un tipo de criminales de cuello blanco, que utilizan sus conocimientos (muy superiores a la media en materia de informática), debemos tener en cuenta, qué tipo de usuarios son los realmente peligrosos como tal. Para ello, podemos englobar a los atacantes según sus conocimientos, en cuatro grupos:

Tipo 1: Son el 85 % de los nuevos intrusos, usuarios de ordenadores, generalmente adolescentes, que encuentran documentación y herramientas en Internet y las ponen en uso, en muchas ocasiones sin tener muy claro el porqué ni el cómo funcionan las aplicaciones que están utilizando y sin saber muy bien lo que están haciendo. Por diversión o en grupos de amigos, y con la ayuda de dichas herramientas, acceden a

[6] Carlos Míguez Pérez, Justo Pérez Agudín y Abel Mariano-Matas García, "La Biblia del Hacker" – Editorial Anaya, 2003 Madrid – Págs. 58 y 59

ordenadores y sistemas que presentan ciertas vulnerabilidades. Este tipo de atacantes, debido a la sofisticación de las herramientas que utilizan, han sido considerados en muchos círculos como la amenaza más preocupante, pues su número empieza a ser tan alto y el nivel de seguridad es tan débil en general, que su persecución y detención es prácticamente imposible con los recursos actuales.

Tipo 2: El 10 % son usuarios más sofisticados que, aunque no suelen saber programar, si han aprendido a compilar algunos códigos fuente de exploits [7] para reventar diversos ordenadores que se encuentran por la red. Además, gracias a las horas de navegación que llevan a cabo con gran interés, han llegado a interpretar muy bien los resultados del conjunto de herramientas que utilizan, lo que convierte sus ataques, de manera individual, en un peligro importante para usuarios, empresas u organizaciones.

Tipo 3: El 4 % de los usuarios que tienen conocimientos profundos en la materia, definen muy bien sus objetivos, cuentan con la destreza necesaria para ingresar en los sistemas, observan y ven lo que quieren o necesitan y efectúan borrados de huellas para evitar ser descubiertos por las herramientas de detección de intrusos o los propios administradores.

Tipo 4: El 1 % son los cibercriminales, individuos con los mismos conocimientos que los englobados en el tipo 3, pero que cometen acciones delictivas a sueldo para terceras personas, organizaciones o para beneficio propio. [8]

Cabe preguntarse si el verdadero "hacker" criminal de cuello blanco, debe seguir siendo sólo el que se corresponde con el Tipo 4, o si también debe incluirse en el grupo a los del Tipo 1, que provocan pérdidas millonarias cada año a muchas empresas y organizaciones, la mayoría de las veces por pura diversión o buscando notoriedad (es el caso de los adolescentes que cada año crean y distribuyen virus que se hacen famosos gracias a su complejidad, al daño que provocan y a la dificultad para eliminarlos).

---

[7] Exploits: Son programas para un determinado sistema operativo que se encargan de explotar ciertas vulnerabilidades de seguridad, con el fin de conseguirle al intruso que lo utiliza los privilegios de súper usuario (más conocido como administrador del equipo).

[8] Carlos Míguez Pérez, Justo Pérez Agudín y Abel Mariano-Matas García, "La Biblia del Hacker" – Editorial Anaya, 2003 Madrid – Pág. 45

Quizás el hecho de que haya unos pocos que tienen conocimientos elevados y participen activamente en grupos de crimen organizado sea un problema, debido a lo difícil que resulta rastrear y detener a personas tan aventajadas en cuanto a conocimientos informáticos, pero también hay que tener en cuenta que los sujetos que por curiosidad, venganza e incluso aburrimiento, utilizan herramientas al alcance de cualquiera (que se pueden encontrar en la red o en libros) para causar daños en otros sistemas, suponen una verdadera bomba de relojería, infravalorada por la mayoría de las personas.

Cabe destacar que el verdadero hacking en sí no debe suponer ningún daño para el usuario de otro equipo o administrador de una página web, pues simplemente consiste en una forma de investigación con el fin de aprender. Todas aquellas formas de hacking dañinas son rechazadas por la comunidad de hackers, ya que manchan su reputación y confunden a la gente acerca de la labor que los verdaderos hackers desempeñan.

Por ejemplo, hoy en día, gracias al desarrollo del software libre y a la proliferación de sistemas operativos gratuitos (como las múltiples distribuciones de GNU- Linux), se está dando a conocer el, hasta ahora casi desconocido, *hacking ético*, en el que muchas personas como las descritas por Raymond se unen para ofrecer al público general aplicaciones seguras, fáciles de utilizar y lo más importante de todo: Gratuitas y libres. Esto último quiere decir que cualquiera puede descargarlas sin pagar ninguna licencia y obtener actualizaciones gratuitas siempre que quiera; y en cuanto a aquellas personas que tengan unos conocimientos mínimos de diseño o programación, pueden modificarlas a su gusto, corregir errores (“bugs”) e incluir nuevas funcionalidades y compartirlo con todo el mundo.

Algunos hacker también son contratados por grandes compañías para desarrollar y comprobar la seguridad de los productos a los que se dedican (como software, antivirus, servicios de hosting o de correo, servidores y páginas web, etc.); e incluso los hay que se unen a los servicios policiales de todo el mundo para ayudar a mantener la seguridad en Internet y luchar contra los delitos informáticos.

La ciencia.

Los hombres de ciencia, especialmente del siglo XVIII en adelante, han gozado de una posición distinguida dentro de nuestra cultura, se han beneficiado de ser figuras de autoridad intachables y han obtenido el respeto instantáneo del común de los mortales.

Se les tiene, por regla general, por personas muy trabajadoras que sacrifican sus vidas al servicio de los ciudadanos del mundo, ataviados con sus impecables batas blancas y con el fin de procurarnos una mejor existencia.
Todo buen investigador espera que algún día, la comunidad científica reconozca sus esfuerzos y descubrimientos otorgándole un Premio Nóbel.

Pero de vez en cuanto, algo llamado fraude científico amenaza con salpicar las batas blancas... Se sostiene que en el mundo científico, al igual que en muchos otros campos, campan a sus anchas individuos débiles o que no tienen escrúpulos, a los que se denomina comúnmente "manzanas podridas".

Charles Babbage fue una de las primeras personas en preocuparse por este fenómeno, y ya en 1830, realizó un estudio para intentar explicar el móvil por el cual los hombres a los que consideraba garantía de verdad, también engañaban. [9]

Sería lógico pensar que las falsificaciones en materia científica son obra de personas con poco renombre que intenta escalar posiciones, pero la historia nos demuestra que los mayores escándalos se encontraron detrás de los mayores científicos del mundo y que se han dado casos de fraude entre nombres tan conocidos como Galileo, Newton, Einstein o Freud.
Uno de los engaños más comunes es la presentación de informes sobre temas que en realidad, no se han investigado en modo alguno, para así evitar perder tiempo o para convencer a la gente de algo que no es posible de una manera práctica. Por ejemplo, se tienen pruebas de que Galileo no llevó a cabo experimentos que el mismo describió y que hoy en día se siguen considerando pilares de la ciencia moderna. Cabe destacar que cuando algunas personas comenzaron a hacer correr rumores y a acusar a Galileo de no haber realizado uno de sus famosos experimentos, el lo admitió, pero aún así, siguió

[9] Federico di Trocchio, "Las mentiras de la ciencia" – Editorial Alianza, 1993 Milán – Pág. 407

defendiéndose diciendo "*Yo, sin hacer el experimento, estoy seguro de que el efecto tendrá lugar como os digo porque es necesario que así ocurra".* [10]

Pero hay algo aún peor que proclamarse el autor de una teoría que no se ha probado e intentar presentarla como verdadera; aquellos científicos, que sin importarles si su descubrimiento es cierto o no, emplean sobornos, amenazas o engaños como medio para hacerse con el tan deseado Nóbel (y la correspondiente y cuantiosa financiación que ello supone).

Existen muchos ejemplos al respecto, pero me parece interesante exponer el caso de Waksman por contener varios elementos: En 1952 Selmann Waksman recibió el premio Nóbel por el descubrimiento de la estreptomicina. En esa época, el único antibiótico conocido era la penicilina, que se generaba a partir de un moho. Como Waksman era microbiólogo, decidió investigar otro tipo de mohos y hongos con el fin de encontrar otro tipo de antibiótico. Uno de sus estudiantes, Albert Schatz, descubrió que un hongo llamado Streptomyces producía un antibiótico que mataba las bacterias causantes de la tuberculosis. Waksman, abrumado por este descubrimiento, consiguió toda la información que necesitaba de su alumno, escribió un artículo en el que figuraba él como jefe del proyecto y Schatz como su ayudante y lo publicó. A pesar de llevar el nombre de los dos hombres, sólo Waksman recibió el Nóbel. Rápidamente patentó la estreptomicina, que le procuró cuantiosas ganancias por parte de la industria farmacéutica.

Schatz, indignado ante los acontecimientos, demandó a su maestro, pero no contaba con la persona de gran influencia y poder en que se había convertido Waksman desde la entrega del premio, que influyó en la comunidad científica para que le reprochasen a Schatz su comportamiento y su falta de respeto hacia el hombre que había sido su mentor.

A partir de este punto, la historia se vuelve algo turbia, y sólo se tiene claro que Schatz fue expulsado de la universidad donde realizó su descubrimiento, que no fue admitido en ninguna otra y que fue rechazado de todos los posibles trabajos que tuvieran que ver con el mundo de la ciencia. Al final, se retiró a Sudamérica donde pasó sus días como profesor de instituto. Algunos dicen que fue Waksman y su omnipotencia, el que relegó a Schatz al olvido de la comunidad científica y que gracias a sus grandes influencias,

[10] Federico di Trocchio, "Las mentiras de la ciencia" – Editorial Alianza, 1993 Milán – Págs. 21 y 22

impidió que el verdadero descubridor de la estreptomicina encontrara trabajo como científico. [11]

Hay múltiples ejemplos de maestros que han robado trabajos y descubrimientos a sus discípulos en el mundo de la ciencia, así como hombres respetables que han recibido el Nóbel gracias al trabajo de su hermana o incluso su hija.

No obstante el mundo de la ciencia cuenta entre sus filas con muchas *manzanas podridas*, cuyo mayor crimen consiste en el desprestigio que suponen para los buenos científicos.

Por todo lo anterior, es de vital importancia, poner en duda también a aquellas personas con buena reputación o que se supone que deben llevarnos a la verdad (como es el caso de los científicos). Las personas que por el simple hecho de ejercer la profesión de médico, matemático o físico, y cuentan con el respaldo de una comunidad que cree en ellas, se exponen muchas veces a un ambiente, en el cual los individuos que buscan un beneficio personal o incluso la derrota de un rival, pueden crecer hasta convertirse en criminales de cuello blanco a los que nadie imaginaría como tal.

[11] Federico di Trocchio, "Las mentiras de la ciencia" – Editorial Alianza, 1993 Milán – Págs. 42 y 43

Las multinacionales.

Desde que existen las empresas, pero sobretodo desde el momento en que la mayoría ampliaron sus mercados a un nivel internacional, la criminalidad de cuello blanco ha ido de la mano de ciertos Directores, altos ejecutivos e incluso de simples trabajadores, que han contribuido en mayor o menor medida a incrementar los beneficios de la compañía para la que trabajan por medios más que dudosos.

Dado que hay múltiples tipos de empresa y que los ejemplos acerca de la criminalidad de cuello blanco en los mercados de todo el mundo son innumerables, resumiremos el tema por medio de un caso conocido.

La multinacional Monsanto, llegó a ser el segundo productor mundial de agroquímicos, así como uno de los principales proveedores de semillas del planeta. Pero si hay algo por lo que es conocida esta compañía, es por ser la productora del herbicida más famoso de la historia: Round Up.
Para muchos, la publicidad con la que Monsanto pretende presentarse como una empresa a favor del medio ambiente y que vende productos que no lo dañan, no es más que una máscara detrás de la cual se esconde la verdadera naturaleza criminal de esta empresa. [12]

Todo comenzó con el gran éxito del herbicida Round Up, que Monsanto presenta como una forma de "control duradero y fiable de malas hierbas anuales y perennes" válido para varios tipos de cultivo. Se debe rociar entre las plantas del cultivo pero sin emplearlo sobre ellas, a fin de matar las malas hierbas que crecen entre las hileras de las plantaciones.

Pronto, el herbicida fue un éxito, ya que verdaderamente era muy efectivo, y los agricultores comenzaron a utilizarlo cada vez más; eso provocó que la manera de utilizar el producto quedase obsoleta, pues cada vez había campos más grandes y era imposible aplicar el herbicida de manera general sin dañar los cultivos.

[12] Fernando Glenza, "Transgénicos: El prontuario criminal de Monsanto" – Agencia Prensa Mercosur

A mediados de los 90, y basándose en la tecnología de modificación genética, comenzó lo que hoy se conoce como "Revolución genética". Monsanto, aplicó esta nueva tecnología para modificar genéticamente las semillas que vendía, para que fueran resistentes al Round Up y poder vendérselas a los agricultores para que pudieran fumigar a gran escala sin preocuparse de sus cultivos... Y lo que aparentemente parecía la maniobra visionaria de la empresa, se convertiría en uno de los mayores crímenes de cuello blanco del mundo empresarial: Monsanto patentó sus semillas genéticamente modificadas como si se tratase de un herbicida más. Esto daría lugar a multitud de conflictos con los agricultores de todo el mundo.

Al patentar las semillas, Monsanto no sólo podía venderlas como si se tratase de un herbicida, sino que también tenía el derecho a demandar a todo aquél que tuviese semillas resistentes al Round Up y que no apareciese en su larga lista de clientes.

Algunos agricultores que jamás habían comprado semillas de Monsanto porque usaban las suyas propias (o las que habían heredado del negocio de agricultura de sus padres), se vieron ante un serio problema cuando en sus campos comenzaron a aparecer plantas que eran inmunes a los efectos del Round Up.
Tras mucho fumigar, algunos agricultores habían conseguido (involuntariamente) que parte de sus cultivos se volvieran resistentes al herbicida. Otros, que tenían sus campos junto a una carretera por la cual solían pasar camiones con semillas o cultivos recogidos, se habían sorprendido cuando descubrieron que la parte de los cultivos colindante con dicha carretera era inmune al Round Up. Por último, está el caso de aquellos agricultores que simplemente se encontraron sus campos contaminados con plantas inmunes al Round Up.

Fue entonces cuando Monsanto comenzó a demandar a todos aquellos pequeños agricultores que supuestamente habían violados las leyes de su patente, siendo común entre ellos las pocas ayudas gubernamentales con las que contaban para la manutención de sus negocios, haber heredado el oficio de su familia y utilizar semillas producidas o bien por sus familiares, o por ellos mismos, o bien compradas fuera del país (incluso en otro continente).

Las preguntas que cabe hacerse acerca de este ejemplo para entender bien la cuestión que nos ocupa son varias.
En primer lugar debemos ocuparnos de si es lícito patentar algo que uno no ha creado (no se puede crear un gen, a todo caso se puede descubrir para qué vale o qué efectos tiene en cierta planta). Monsanto utilizó el tamaño, la fama y los recursos económicos de los que disponía, para comprar (literalmente) al laboratorio que realizó las pruebas genéticas con los cultivos y así poder hacerse con el descubrimiento (que no invento) del gen que inmuniza a las plantas contra el Round Up.

En segundo lugar (y seguramente aquí se encuentra el quid de la cuestión), ¿cómo es posible que Monsanto supiera qué agricultores tenían plantas inmunizadas?
Para saber si una planta es inmune al Round Up, sólo se pueden hacer dos cosas: Aplicarle directamente el producto (con lo que se corre el riesgo de matarla) o analizar una muestra genética en un laboratorio. Monsanto no tenía ninguna razón para analizar cultivos al azar de pequeños agricultores que ni siquiera eran sus clientes en lo que a semillas se refiere... ¿No es sospechoso que una empresa obtenga muestras de un campo (¡sin permiso de su dueño!) para practicar sobre ellas un análisis de laboratorio que permita saber si son inmunes al Round Up?

La tercera cuestión: Los agricultores, así como muchos investigadores, personal de justicia implicado en las demandas de Monstanto y ecologistas, creen que la propia empresa se dedicó a infectar campos de agricultores que no compraban sus semillas, para poder demandarles por violar la patente después.
Monsanto cuenta con innumerables procesos judiciales a sus espaldas, y aún hoy en día muchas de esas disputas siguen abiertas, lo cual está empobreciendo y arruinando a muchos pequeños agricultores que tuvieron la mala suerte de cruzarse en su camino con un gigante de la industria.
Aún en el caso de que Monsanto no infectase los campos de sus “rivales”, el viento y los insectos pueden “infectar” de manera natural los campos que no contienen las semillas modificadas.
Muchos consideran un verdadero crimen el trato de Monsanto hacia los agricultores, puesto que les obliga a pagar una multa que la mayoría no pueden pagar, así como arruina sus negocios familiares al dejarles sin semillas propias (ya que las

genéticamente modificadas son más resistentes y por ende, tienen más posibilidades de sobrevivir).

El paso final de toda esta cadena es conseguir un monopolio absoluto sobre las semillas que se plantan en cada campo. Tanto si un agricultor es cliente de Monsanto como si no, acabará por tener plantas inmunes al Round Up en sus cultivos, ya sea por acción del viento, por los insectos, por un camión que pasa cerca dejando caer restos de cultivos o porque los empresarios de Monsanto infectan su campo cuando nadie les ve (teoría algo rebuscada, pero posible).

Volviendo al tema de la criminalidad de cuello blanco, cabe destacar que entre las empresas más poderosas del mundo se encuentran las petroleras, las farmacéuticas, las tabacaleras y las empresas de productos agrícolas como Monsanto, y que en todas ellas se han dado este tipo de comportamientos en mayor o menor medida, haciéndole sombra incluso a los grupos dedicados al crimen organizado.

Conclusiones.

Ya hemos visto tres buenos ejemplos de conductas que no están abiertamente consideradas como criminalidad de cuello blanco, especialmente desde el punto de vista de la opinión pública debido principalmente al desconocimiento o la falta de atención de los medios de comunicación hacia estos temas.

En el caso del hacking, hemos visto que no todos los tipos de hacking son dañinos y que hay un enorme volumen de personas accediendo a herramientas e información gratuitas que pueden dañar o destruir muchos equipos, páginas web o redes sin demasiada dificultad y sin ser considerados un verdadero problema cuando hablamos de seguridad informática.
También hemos visto algunos ejemplos acerca de cómo los hombres de ciencia son muchas veces inmunes a ser tachados de criminales de cuello blanco, a pesar de haber cometido actos impropios de lo que debiera ser un buen científico o cualquier otra personalidad importante en el campo de la investigación.
Por último, centramos nuestra atención sobre las grandes multinacionales que utilizan métodos agresivos contra personas u otras empresas más pequeñas, con el fin de aumentar sus ingresos, conseguir dominar el mercado, etc., y todo ello con una casi total impunidad.

¿Qué diferencia a los criminales de cuello blanco y a los sujetos que hemos empleado como ejemplo en este trabajo?
Si recordamos las características que tienen en común los distintos criminales de cuello blanco, veremos que tanto los hackers maliciosos como algunos científicos, así como ciertas multinacionales, reúnen dichas características en su modus operandi, y por lo tanto, podemos afirmar que hay otras formas de criminalidad de cuello blanco que no están lo suficientemente estudiadas como para ser consideradas como tal y reconocer abiertamente, que no sólo de empresarios poderosos o de gente adinerada se alimenta el amplio elenco de criminales de cuello blanco.

Después de haber recorrido el camino que nos ocupa a lo largo de este trabajo y partiendo de la definición de criminal de cuello blanco de Sutherland, podemos redefinir a este tipo de delincuentes para adaptar el concepto a nuestros días:

Aquellas personas físicas o jurídicas que valiéndose de

- *las habilidades y/o conocimientos que poseen,*
- *la posición social elevada y el respeto de la sociedad,*
- *así como de la importancia, los recursos económicos y la fama que poseen,*

cometen actos abusivos, destructivos o que puedan ser considerados constitutivos de delito, todo ello con el fin de beneficiarse social o económicamente.

De esta manera incluimos en la antigua definición tanto a las personas físicas como a las jurídicas (empresas, instituciones,…), a los que utilizan sus conocimientos y habilidades para provocar un daño sin ser necesariamente acaudalados ni bien reconocidos (como es el caso de muchos crackers o programadores de virus informáticos), a los que se valen de su reconocimiento social o a la fe que depositan en ellos el resto de personas por ser lo que son (como pueden ser los científicos, los religiosos,…) y a aquellos que tienen mucho poder – tanto económico como social – como es el caso de algunas multinacionales.
Aunque se ha ampliado el tipo de actos que pueden ser considerados como criminalidad de cuello blanco (actos abusivos y destructivos), éstos deben tener su correspondiente tipificación en los códigos penales para poder aplicar la ley de una manera efectiva.

También se hace referencia a otros motivos por los que uno puede convertirse en un criminal de cuello blanco, como es el reconocimiento social (que en ciertas ocasiones otorga más beneficios profesionales y económicos pero otras no, como es el caso de algunos jóvenes crackers, que sólo obtienen el reconocimiento de sus amigos más cercanos).

Para terminar me gustaría apuntar que hay infinidad de tipologías de criminalidad de cuello blanco no reconocidas, que no se tratan en este trabajo porque supondría una extensión demasiado larga y una profundidad que requiere muchas horas de investigación; no obstante quisiera citar, con el fin de no dejar cabos sueltos, a los criminales de cuello blanco que se esconden tras muchos Gobiernos y Estados y tras importantes instituciones religiosas de todo el mundo.

El escritor y filósofo Miguel de Unamuno dijo que "*el progreso consiste en renovarse*". Si no queremos que las nuevas formas de criminalidad de cuello blanco o aquellas que no han sido reconocidas como tal hasta el momento, amenacen aún más nuestras sociedades, más nos vale renovar las ideas que tenemos acerca de estos delincuentes: Quiénes son, cómo son, dónde y cómo actúan, y lo más importante de todo, no dejar que lo políticamente correcto constituya un obstáculo a la hora de señalar a personas que hasta ahora, a nadie se le ha ocurrido asociar con la criminalidad de cuello blanco.

Bibliografía.

Recursos empleados para la realización de este trabajo ordenados por temas:

Introducción

* Libros:

- "Estudios de criminalidad económica", Agustín Fernández Albor – Editorial Bosch, 1978 Barcelona, ISBN: 8471627280

El Hacking

* Libros:

- "La Biblia del Hacker", Carlos Míguez Pérez, Justo Pérez Agudín y Abel Mariano-Matas García – Editorial Anaya, 2003 Madrid, ISBN: 8441515387

* Páginas web:

http://www.informatica-pc.net/hackers/hackers.php

http://www.catb.org/hacker-emblem/

http://es.wikipedia.org/wiki/Hacker_de_sombrero_blanco

http://es.wikipedia.org/wiki/Hacker_de_sombrero_negro

http://www.catb.org/~esr/jargon/

La Ciencia

* Libros:

- "Las mentiras de la ciencia", Federico di Trocchio – Editorial Alianza, 1993 Milán, ISBN: 8420639885

Las Multinacionales

* Páginas web:

http://www.aldearural.com/subcategorias/documentacion/monsanto.htm

http://www.combat-monsanto.es/

http://www.monsanto.es/

http://www.thefutureoffood.com/

* Documentales:

- "The future of food", escrito y dirigido por Deborah Koons García.

Bibliografía recomendada por temas:

El Hacking:

- "Hacker: Guía práctica", María Teresa Jimeno García – Editorial Anaya, 2008 Madrid, ISBN: 9788441523234
- "Cracking sin secretos: Ataque y defensa de software", Jakub Zemanek – Editorial Ra-Ma, 2004 Madrid, ISBN: 9788478976287

La Ciencia:

- “El genio incomprendido: Hombres e ideas que la ciencia no ha comprendido”, Federico di Troccio – Editorial Alianza, 1999 Madrid, ISBN: 9788420639703
- “El conocimiento inútil”, Jean François Revel – Editorial Planeta, 1989 Barcelona, ISBN: 8432047899

Las Multinacionales:

- “La mafia médica”, Ghislaine Lanctōt – Editorial Vesica Piscis, 1994 Canadá, ISBN: 8493234923
- “La mafia médico-farmacéutica”, revista The Ecologist (edición para España y Latinoamérica), número 12, 2003, ISSN: 15782964