CYBERINVESTIGACIÓN

Prevención - Represión - Investigación - cybercriminólogo

José Manuel Ferro Veiga

securidas@wanadoo.es

Índice o sumario del libro

Introducción. La conflictividad entre el control empresarial y la intimidad de los trabajadores

El FBI cuenta con un departamento que se dedica únicamente a investigar y perseguir a los delincuentes que actúan en Internet. La agente especial Jennifer Marsh (Diane Lane) creía haberlo visto todo.. Hasta ahora. Un depredador cibernético cuelga torturas y asesinatos en su página web El destino des sus prisioneros depende del público: cuantas más visitas registre su página web, más deprisa morirán las víctimas, Cuando el juego del gato y el ratón se convierte el algo personal, Jennifer y su equipo deberán lanzarse a una carrera contrarreloj para encontrar a este asesino.

Pues bien, esta es la sinopsis de la película Rastro oculto (Untraceable) de origen Estadounidense que nos adentra el mundo del c ybercrimen.

Entre las conductas delictivas que se cometen con más frecuente a través de Internet tienen que ver sobre todo con los siguientes aspectos :

- Menores.
- Amenazas, calumnias e injurias.
- Estafas a través del comercio electrónico.
- Vulneración de derechos de propiedad intelectual e industrial.
- Acceso a datos reservados de carácter personal.
- Acceso a secretos de empresa.
- Daños en sistemas informáticos .
- Venta de productos prohibidos a través de Internet.
- La apología de Terrorismo y la xenofobía.
- Uso ilícito de Internet en el Trabajo

El término "ciberdelito" abarca muy diversos tipos de actividad delictiva, que comprenden una gran variedad de infracciones, lo que dificulta su clasificación, entre otras razones, porque cada día aparecen figuras nuevas. Un sistema de clasificación interesante es el definido por el Convenio sobre la Ciberdelincuencia del Consejo de Europa, en el que se distinguen cuatro tipos diferentes de infracciones, dentro de cada una de las cuales hay, as vez, diversas figuras delictivas.

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

1. Acceso ilícito (piratería de sistemas y programas)

2. Espionaje de datos
3. Intervención ilícita
4. Manipulación de datos
5. Ataques contra la integridad del sistema

Delitos relacionados con el contenido.

1. Material erótico o pornográfico (excluida la pornografía infantil).
2. Pornografía infantil
3. Racismo, lenguaje ofensivo, exaltación de la violencia
4. Delitos contra la religión
5. Juegos ilegales y juegos en línea
6. Difamación e información falsa
7. Correo basura y amenazas conexas
8. Otras formas de contenido ilícito

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Delitos informáticos.

1. Fraude y fraude informático
2. Falsificación informática
3. Robo de identidad
4. Utilización indebida de dispositivos
5. Existe la posibilidad de ampliar esta clasificación, combinando delitos, que se cometen por internet, como: el ciberterrorismo, la guerra informática, el ciberblanqueo de dinero, etc

Resulta difícil cuantificar el número de delitos que se pueden cometer por internet -ciberdelitos- dado que las víctimas no siempre informan de ello. Sin embargo, las estadísticas pueden ayudar a comprender la incidencia de esta actividad delictiva.

Según una Encuesta Mundial sobre seguridad 2011, realizada en 78 países. El 25% de las empresas encuestadas han sufrido ciberataques en el último periodo de doce meses. Este porcentaje se traduce en que una de cada cuatro empresas ha sufrido ciberataques en los últimos doce meses.

Si a nivel empresarial es preocupante el índice de impacto que tiene la ciberdelincuencia, lo es también el que se refleja a nivel usuario de Internet. De un estudio sobre Cibercrimen realizado por SYMANTEC,

(Empresa que comercializa en España los sistemas de seguridad NORTON 360, NORTON ANTIVIRUS Y NORTON INTERNETSECURITY y que cuenta con 300 millones de clientes en el mundo), sobre una muestra de 13.000 internautas adultos en 24 países, refleja que 1 de cada 5 internautas adultos ha sido víctima de al menos un ciberdelito. El estudio también desvela nuevos métodos de cibercrimen basados en las redes sociales y los dispositivos móviles. Asimismo, una de las principales conclusiones de este informe es la afirmación de que el cibercrimen está en auge y, que los cibercriminales buscan el anonimato y el lucro en sus acciones, más que la fama y notoriedad demandada hace unos años.

Algunos de los datos más relevantes del estudio de SYMANTEC, son los siguientes:

Cada segundo, 18 adultos son víctimas de ciberdelitos: es decir, más de un millón y medio de víctimas cada día en todo el mundo.

En los últimos 12 meses, cerca de 556 millones de adultos en el mundo han experimentado algún ciberdelito, cifra que supera a la población total de la Unión Europea.

El 46% de los internautas adultos han sido víctimas del cibercrimen en los últimos 12 meses.

Uno de cada cinco adultos (21%) ha sido víctima o bien de cibercrimen en redes sociales o a través del dispositivo móvil, y el 39% de los usuarios de redes sociales han sido víctimas de cibercrimen social.

El 15% de los usuarios de redes sociales informa que alguien ha accedido sin permiso a su perfil y se han hecho pasar por ellos.

El 10% afirma que han sido víctimas de enlaces fraudulentos en las redes sociales.

El 44% utiliza una solución de seguridad para que los proteja de amenazas en las redes sociales.

El 49% utiliza la configuración de privacidad para controlar qué información comparten y con quién.
Casi un tercio (31%) de los usuarios de móviles recibieron un mensaje de texto de alguien que no conocían pidiendo que accedieran a un determinado enlace o marcasen un número desconocido para escuchar un mensaje de voz.

El 27% de los internautas adultos ha recibido un mensaje diciéndoles que su contraseña del correo electrónico había sido cambiada.

Asimismo, EUROPOL señala que los fraudes con tarjetas de crédito asciende hasta a 1.500 millones de euros anuales (2.000 millones de dólares).

Ni decir tiene que este volumen de actividad delictiva tiene unas importantísimas repercusiones económicas. Se cifra en 338 mil millones de dólares los gastos que produjeron en 2011, los ataque virtuales. Asimismo, se calcula que las pérdidas medias a nivel mundial por víctima son de 152 euros en costes financieros directos.

El número cada vez mayor de ciberdelitos reconocidos y, las herramientas técnicas para automatizar estos tipos de delitos, hace que la lucha contra el ciberdelito se haya convertido en un elemento esencial de las actividades relativas al cumplimiento de la ley en todo el mundo. Es primordial la creación e implementación de una estrategia anticiberdelito eficaz como parte de la estrategia de ciberseguridad nacional. La agenda sobre Ciberseguridad Global basa sus principales objetivos estratégicos en cinco áreas de trabajo, que son:

1. Las medidas legales
2. Las medidas técnicas y de procedimiento
3. Las estructuras institucionales
4. La creación de capacidades
5. La cooperación internacional

Medidas legales. Son probablemente las más importantes con respecto a una estrategia anticiberdelito. Ello requiere en primer lugar la elaboración de unas leyes penales sustantivas necesarias para criminalizar actos tales como el fraude informático, acceso ilegal, interferencia en los datos, violaciones del derecho de propiedad intelectual y la pornografía infantil. El hecho de que existan disposiciones en los Códigos Penales, que son aplicables a actos similares cometidos fuera de la red no significa que puedan aplicarse también a los actos cometidos a través de Internet. Por consiguiente, es muy importante realizar un análisis profundo de las actuales legislaciones nacionales a fin de identificar posibles lagunas jurídicas.

Medidas técnicas y de procedimiento. Las investigaciones relativas al ciberdelito a menudo tienen un fuerte componente técnico. Por consiguiente, el desarrollo de las capacidades y procedimientos necesarios es un requisito esencial en la lucha contra el ciberdelito.

Estructuras institucionales. Una lucha eficaz contra el ciberdelito exige unas estructuras institucionales altamente desarrolladas. Sin contar con las adecuadas estructuras que eviten la duplicación de medidas y se basen en unas competencias claramente establecidas, difícilmente será posible llevar a cabo las complejas investigaciones que exige la asistencia de distintos expertos jurídicos y técnicos.

Creación de capacidad y educación del usuario. Se requiere, particularmente, la educación del usuario. Algunos ciberdelitos, especialmente los relativos al fraude, tales como usurpación de identidad -"phishing"- y falsificación de direcciones de origen o piratería -"spoofing"-, no se producen generalmente debido a la ausencia de protección técnica, sino a causa de una falta de atención por parte de las víctimas.

Cooperación internacional. El ciberdelito es un fenómeno global; para poder investigar eficazmente estos delitos es necesario establecer una armonización de las leyes y desarrollar los métodos adecuados para lograr la cooperación internacional. Cada vez más, los ciberdelitos adquieren dimensión internacional, esto se debe a que prácticamente no es necesario que el delincuente esté físicamente presente en el lugar en que se ofrece un servicio. Por este motivo, tampoco necesitan estar presentes en el lugar en que se localiza a la víctima. En general, en las investigaciones sobre ciberdelitos es imprescindible la cooperación internacional.

El fraude por Internet parece no tener fin y ha llegado incluso a la Administración Pública. Hace un tiempo se conoció un intento de engaño en nombre del Instituto Nacional de Estadística con el fin de recabar datos personales de posibles víctimas; y poco después se supo de la existencia de un correo electrónico simulado, aparentemente enviado por la Agencia Tributaria, en el que se pedía las claves bancarias de los contribuyentes para recibir una supuesta devolución de impuestos de hasta 90 euros.

El Cuerpo Nacional de Policía desarticulo en 2004 una de las mayores redes españolas de tráfico de sustancias estupefacientes y medicamentosas prohibidas. En total fueron detenidas 21 personas que se dedicaban a la distribución y venta clandestina de estas sustancias a través de Internet.

La principal peculiaridad de esta operación, en la que se han efectuado trece registros en toda España, radica en que se trata de la mayor red de traficantes de psicotrópicos, esteroides, anabolizantes y hormonas, que utilizaba Internet para su distribución en territorio nacional y en el extranjero, según informó ayer la Dirección General de la Policía.

Según las fuentes citadas, "miles de clientes" de esta red buscaban aumentar su rendimiento deportivo con sustancias energéticas, para disminuir la fatiga o aumentar la masa muscular, tales como estimulantes, esteroides, anabolizantes androgénicos, anabolizantes y algunas hormonas.

De hecho, la distribución se realizaba en parte a través de personas muy relacionadas con gimnasios, a las que resultaba "sumamente fácil" la venta entre clientes que buscaban progresos rápidos en la musculación y que consumían dichas sustancias sin control médico alguno.

Cuatro de las detenciones se practicaron en Málaga, otras cuatro en la provincia de Madrid, dos en Barcelona, tres en Zaragoza, dos en O Porriño (Pontevedra), dos en Tarragona, una en Calpe (Alicante), y dos en Gandía (Valencia).

Todos los detenidos (18 españoles, un tunecino, un ecuatoriano y un venezolano) pertenecen a los "escalones superiores" de esta red, explicó la Policía Nacional, que subrayó que la operación sigue abierta y que continuará con los "escalones inferiores" de la organización.

Anonimato

La red, de carácter nacional y cuyos integrantes creían garantizado su anonimato mediante el uso de comunicaciones a través de Internet, estaba dedicada al tráfico ilícito de psicotrópicos (principalmente GHB) y precursores de sustancias estupefacientes, como la efedrina.

Los detenidos compraban gammahidroxibutirato (GHB) y lo distribuían y vendían al por menor, con las instrucciones y el material necesario para la elaboración de éxtasis líquido. Además, distribuían de forma ilícita sustancias medicamentosas, incluidas algunas especialidades de uso veterinario (como esteroides, anabolizantes, hormonas y clembuterol), orientadas al consumo humano.

Los distintos escalones de la organización se comunicaban a través de Internet, y usaban la Red para las transacciones económicas, aunque algunas ventas se pagaban con ingresos en cuentas bancarias (a veces a nombre de terceras personas) y, cuando era una cantidad importante, en contactos "cara a cara".

Las investigaciones comenzaron , cuando la Brigada de Investigación Tecnológica de la Policía comprobó que un individuo había invadido

multitud de páginas web con anuncios en los que ofertaba estas sustancias, y se centró en un grupo de españoles, dirigido por un estudiante de la Facultad de Medicina de Málaga.

Esta persona, que estableció contactos en Argentina, EE.UU., Italia, Chile, México y Tailandia, usaba diversas medidas de seguridad para garantizar su impunidad en Internet, y distribuía las sustancias a través de empresas de paquetería.

Sin embargo, las gestiones posteriores demostraron la existencia de un escalón superior en la organización compuesto por tres individuos residentes en Portugal, Galicia y Málaga.

Lacra social

Para Jaime Lissavetzky, exsecretario de Estado para el Deporte, las redes de tráfico y distribución de sustancias dopantes son "una lacra social", y aseguró que, tanto si trabajan con deportistas profesionales como si lo hacen en gimnasios, "la tolerancia será cero". Añadió que "son personas que hacen daño a los demás. Esas sustancias perjudican gravemente la salud".

El abuso de sustancias anabolizantes para ganar masa muscular y el seguimiento de dietas estrictas sin más fundamento que la obsesión por limitar al máximo las grasas y preponderar las proteínas son rasgos comunes entre las personas afectadas por vigorexia. Es un trastorno psicológico que afecta sobre todo a hombres jóvenes, de entre 18 y 35 años, que acuden a diario al gimnasio para ganar masa magra con ejercicios de musculación y pesas.

La presión social hacia un cuerpo bello, esbelto y delgado en las chicas, y apuesto y musculoso en los chicos, influye sobremanera en la percepción de la propia imagen real y tiene una incidencia expresa en la conducta y en el comportamiento alimentario. Esto determina que algunas personas desarrollen rasgos obsesivos en la selección y consumo de alimentos que, a medio y largo plazo, pueden desencadenar trastornos más serios como los diagnósticos de anorexia y bulimia nerviosa u otros nuevos desórdenes alimentarios, como el trastorno por atracón, la ortorexia o la diabulimia. Si la obsesión se centra en ganar músculo mediante la práctica de ejercicio y éste es desmesurado tanto en la ejecución como en la intensidad y la frecuencia, el diagnóstico está claro: dismorfia muscular, más conocida como vigorexia.

Dieta extrema y abuso de sustancias

No hay, por el momento, estudios epidemiológicos, aunque sí estimaciones, sobre personas que podrían cumplir el diagnóstico de vigorexia, un trastorno de índole psicológica. El informe "Ortorexia y vigorexia: ¿nuevos trastornos de la conducta alimentaria?", de las psicólogas Rosario Muñoz y Amelia Martínez, relata que en España unas 20.000 personas sufren vigorexia, lo que supone 1 de cada 2.000 personas. De ellas, el 80% son hombres.

Aunque se denomina "la anorexia de los 90", es un trastorno distinto, no estrictamente alimentario, si bien comparte la preocupación enfermiza por la figura y una distorsión de la imagen corporal. El miedo a estar obeso y una preocupación exagerada por la apariencia física, junto con el deseo siempre presente de ganar masa magra y ajustarla al máximo, propicia que el individuo se obsesione con la práctica de ejercicio y recurra a los ejercicios de musculación y pesas durante varias horas al día, en su mayoría, todos o casi todos los días de la semana. Los afectados se pesan varias veces en una sola jornada y se comparan con otros compañeros de gimnasio. El trastorno deriva en un cuadro obsesivo-compulsivo que favorece que se sientan fracasados, abandonen sus actividades y se encierren en gimnasios durante varias horas.

La conducta obsesiva se refleja también en una excesiva atención a la dieta, que se caracteriza por un consumo exagerado de alimentos proteicos ante la creencia incierta de que la proteína beneficia al músculo. Las tortillas de claras y las pechugas de pollo, además de proteína en polvo a cucharadas, son los componentes diarios en la dieta, que es desequilibrada en su conjunto, monótona y poco o nada apetitosa.
A esta particular dieta hiperproteica, popular entre asiduos a gimnasios y quienes practican con pesas, se añade el consumo de sustancias peligrosas con una función, en teoría, "quemagrasas" y que aumenta (de manera artificial y descomunal) la masa muscular, como son hormonas y anabolizantes esteroideos.

El mayor peligro radica en que tras el nombre de complementos dietéticos para la nutrición deportiva, como complejos vitamínicos o de minerales, ayudas ergogénicas para aumentar la energía muscular (carnitina, creatina), suplementos proteicos o batidos, entre otros, se pueden enmascarar sustancias diuréticas y anabolizantes cuyo consumo mantenido y sin control médico puede provocar graves problemas de salud. Rosario Muñoz y Amelia Martínez completan su informe con datos de otro análisis de la Comisión Europea que reflejan cómo "un 6% de las personas que acuden a un gimnasio se dopan, es decir, consumen