Revista de Derecho UNED, núm. 12, 2013

LOS NUEVOS MODI OPERANDI DE LOS CIBERDELINCUENTES DURANTE LA CRISIS ECONÓMICA

THE NEW MODI OPERANDI OF CYBERCRIMINALS DURING THE ECONOMIC CRISIS.

Juan de Dios Meseguer González

Abogado en ejercicio. Perito Informático Judicial. Doctorando en Derechos Fundamentales en la UNED (Curso 2012/2013)

Resumen: Con el presente artículo, pretendemos dar a conocer el conflicto y los retos tanto policiales como procesales, para hacer frente a un variado e innovador tipo de delincuencia que atenta constantemente **«desde el lado oscuro de la red»** a los Derechos Fundamentales de nuestros ciudadanos, pero que de manera especial, en los años que llevamos de crisis[1] económica, se ha incrementado sustancialmente. Para ello, hemos realizado un estudio técnico informático y procesal penal[2], de los fenómenos afectados.

Nuestro estudio que se basa fundamentalmente en la experiencia profesional adquirida durante los años precedentes, en contacto con los distintos fenómenos analizados, se sustenta no solo en la investigación sobre fenomenología, sino que además, se sirve de las posturas de quienes, en las áreas tratadas, son especialistas en la materia.

[1] SALGADO, Víctor. «*La crisis no sólo no frena el desarrollo de lo Sociedad de la Información sino que la acelera*». Entrevista: http://issuu.com/parnet-tic/docs/boletin_n19_final_120ppp

[2] ROMEO CASABONA, Carlos María. «*El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*». 1.ª ed., 1.ª imp. Septiembre 2006.

Todo ello, para mostrar un trabajo que pretende una exposición específica para el modelo que afecta al código penal español[3], siendo conscientes que el estudio no se limita a los conceptos y términos desarrollados, porque para un mayor alcance de la fenomenología analizada, hubiera hecho falta relacionarlo con otros modelos internacionales, al trascender este tipo de delitos y crímenes, las fronteras de los Estados. No obstante, este estudio se concreta por motivos de espacio y objetivos, a la extensión que presentamos.

Este artículo tiene tres partes bien diferenciadas. En **primer lugar** introduce y diferencia una serie de términos relacionados con el fenómeno del ciberdelito y la seguridad cibernética.

En **segundo lugar**, se lleva a cabo un desarrollo desde un punto de vista técnico informático, para tratar la problemática emergente que supone una serie de fenómenos, para los que no existe una concienciación social precisa en nuestra sociedad y que exige una respuesta inmediata y coordinada de todos, para que se adopten las medidas necesarias, no solo por los fans de las redes sociales, sino también por cualquier ciudadano de a pie que use las nuevas tecnologías para usos personales: buscar empleo, llevar a cabo transferencias u operaciones por la web, etc; dado que existe un alarmante crecimiento del modus operandi del ciberdelincuente en el 2012.

En **tercer lugar**, analizamos cuales pueden ser los métodos más eficaces desde el punto de vista jurídico penal[4], para combatir y frenar estos ilícitos cibernéticos[5].

Finalizaremos nuestro estudio, con unas conclusiones.

Abstract: With this article, we aim to raise awareness of the conflict and the challenges both police procedural, to address a varied and innovative type of crime that threatens constantly «from the dark side of the network» fundamental rights of our citizens, but especially so in the years we have economic crisis, has increased substantially. To do this, we studied computer technician and criminal procedure of the phenomena involved.

[3] https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/normativa_estatal/common/pdfs/E.2-cp-C-oo-digo-Penal.pdf

[4] PÉREZ GIL, Julio. «*El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito*». Ed. La Ley, Madrid 2012.

[5] McAfee: «*La recesión económica es un semillero para la actividad fraudulenta pues los delincuentes cibernéticos se aprovechan del clima de miedo y ansiedad que hay entre los consumidores*». *http://www.eluniversal.com.mx/articulos/51700.html*

Our study is based primarily on the experience gained during the previous years, in contact with the various phenomena analyzed, is based not just on research on phenomenology, but also uses the positions of those in the treated areas are specialists in the field.

All this, to show work that seeks a specific exposure to the model affects the Spanish penal code, be aware that the study is not limited to developed concepts and terms, because for a greater range of phenomenology analyzed, would have needed relate with other international models, to transcend these offenses and crimes, the State boundaries. However, this study is specific for space reasons and objectives, to the extent that we present.

This article has three distinct parts. First introduced and unlike a number of terms related to the phenomenon of cybercrime and cybersecurity.

Second, it performs a development from a technical standpoint computer, to treat emergent problems involving a series of phenomena, for which there is no precise social awareness in our society and that requires immediate and coordinated response of all, to adopt the necessary measures, not only for fans of social networking, but also for any ordinary citizen to use new technologies for personal: find a job, perform transfers or transactions the web, etc., since there is an alarming growth of cyber criminal modus operandi in 2012.

Third, we analyze what may be the most effective from the point of view of criminal law to combat and stop these illegal cyber.

Finally we study with conclusions.

Palabras clave: Ciberdelitos, Cibercrímenes, Ciberdelincuentes, Ciberterroristas, crimeware, redes sociales, malware, falsos programas antivirus, Fraudes, tratamiento jurídico penal.

Keywords: Cybercrime, Cybercrime, cyber criminals, cyber terrorists, crimeware, social networks, malware, scareware, fraud, criminal legal treatment.

Recepción original: 17/03/2013
Aceptación original: 25/04/2013

I. INTRODUCCIÓN. DIFERENCIACIÓN DE CONCEPTOS

Con carácter previo, creemos que es preciso distinguir brevemente, dos conceptos que hemos observado se suelen emplear indistintamente y erróneamente en muchos estudios, por algunos autores que aparecen en internet o en otras publicaciones, confundiendo los objetivos y finalidades de ambos.

Nos referimos concretamente a los conceptos[6] de Ciberdelitos y Cibercrímenes respectivamente, como aquellas figuras que muestran su similitud entre delitos y crímenes, pero que se desarrollan en el Ciberespacio, red informática y que pueden afectar a los servicios de internet. La confusión viene, porque se utiliza por igual Ciberdelitos como Cibercrímenes[7].

Si bien, no es incorrecto hacerlo en términos generales, dicha terminología se muestra como imprecisa a la hora de clasificar y distinguir las distintas figuras: Ciberdelincuentes y Ciberterroristas[8]. En este sentido, los ciberdelitos se incluirían de manera más exacta dentro de las actividades de los ciberdelincuentes, definidos como actividades genéricas y menos graves: el fraude informático[9], el robo, la falsificación, el scammer[10], el computer hacking, el espionaje informático, el sabotaje y extorsión informáticos, la piratería comercial y otros tipos ilícitos contra la propiedad intelectual, la invasión de la intimidad[11], la distribución de contenidos ilegales y dañosos, la incitación a la prostitución y otros crímenes contra la moralidad.

[6] MAGLIONA MARKOVICH, Paul Claudio; LÓPEZ MEDEL, Macarena. «*Delincuencia y fraude informático*». Derecho comparado y Ley 19223. Ed. Jurídica de Chile. 1999.

[7] ROGRÍGUEZ BERNAL, Antonio. «*Los cibercrímenes en el espacio de libertad, seguridad y justicia*», en Revista de Derecho Informático, no. 103, febrero 2007, págs. 1-42.

[8] JORDÁN, Javier y TORRES, R. Manuel. «*Internet y actividades terroristas: el caso del 11-M*», en El profesional de la información, v. 16, n. 2, marzo-abril, 2007, págs. 123-130.

[9] GUTIÉRREZ FRANCÉS, M. L., «*En torno a los fraudes informáticos en el derecho español*», que conviene no confundir el fraude informático con el delito informático, esto es, la parte con el todo, puesto que aquél no es más que un tipo de delincuencia informática, en AIA, núm. 11, abril, 1994, pág. 7.

[10] SCAMMERS: las estafadoras del amor. La palabra «scammer» significa «estafador» o «estafadora». Las scammers se aprovechan de un mal endémico en la sociedad: la soledad. En los últimos años, se ha ido incrementado el número de personas que se inscriben a portales que ayudan en la búsqueda de pareja, como Meetic.

[11] ÁLVAREZ-CIENFUEGOS SUÁREZ, J. «*La defensa de la intimidad de los ciudadanos y la tecnología informática*». Editorial Aranzadi S.A., Pamplona, 1999.

Frente a estos nos encontramos con el cibercrimen[12], como los delitos más graves, como los provenientes de los ciberterroristas[13], por la convergencia del ciberespacio y el terrorismo, forma en la que el terrorismo utiliza las tecnologías de la información para intimidar, coaccionar o para causar daños a grupos sociales con fines políticos-religiosos.

En definitiva, que dentro también del cibertorrorista como cibercriminal y cuyos objetivos principales son ocasionar miedo, destrucción y daño, de manera amplia a las personas, más allá del fraude o el chantaje en si mismo considerado, porque afectaría a la vida y seguridad de las mismas tanto a nivel nacional como internacional: los ilícitos cometidos atentando a centrales nucleares, medios de transporte aéreos, gaseoductos, centrales eléctricas, etc.

Ambos conceptos, se presentan como dos fenómenos con características similares en cuanto a ciertas técnicas para vulnerar los sistemas informáticos, pero distintas y complejas en cuanto al fin último perseguido.

II. EL IMPACTO DE LOS CIBERDELINCUENTES EN LAS REDES SOCIALES

Según los estudios avalados por distintas empresas dedicadas a la seguridad (por citar las más conocidas a nivel de usuario): NORTON[14], KASPERSKY[15], HP[16], así como otras grandes empresas de las telecomunicaciones: CISCO[17], Microsoft[18], etc; este año, es el **tercer año consecutivo, en el que los ciberdelitos han seguido aumentando**[19].

En concreto, la incidencia de los ataques cibernéticos[20] ha crecido más del doble, mientras que el impacto que a nivel financiero esto ha repercutido en un incremento del casi 40% para el año 2012. Esta es

[12] LARKIN, Eric. «*Cibercrimen (I): Delincuentes profesionales online*», en PCWorld, n.º 224, 2005, págs. 26-30.

[13] ORTA MARTÍNEZ, Raymond. «*Ciberterrorismo*», en Revista de Derecho Informático, no. 082, mayo 2005.

[14] http://www.symantec.com/es/es/index.jsp

[15] http://www.kaspersky.com/sp/

[16] http://www8.hp.com/es/es/home.html

[17] http://www.cisco.com/web/learning/netacad/index.html

[18] http://www.microsoft.com/es-es/default.aspx

[19] Principales datos y conclusiones de la tercera edición del «*Estudio sobre el cibercrimen 2012*», conducido por el Instituto Ponemon y patrocinado por HP Enterprise Security.

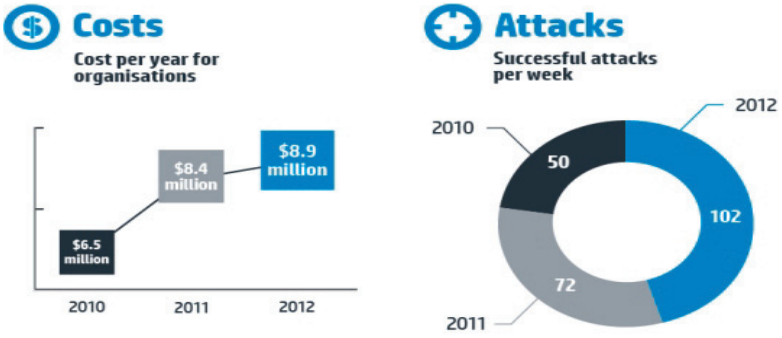
[20] Facebook y Twitter protagonizaron la mayoría de ataques cibernéticos de 2012. http://www.republica.com/2013/01/13/facebook-y-twitter-protagonizaron-la-mayoria-de-ataques-ciberneticos-de-2012_600061/

una realidad, que nos permite hablar, que hemos pasado de la propagación de «**los virus a la ciberdelincuencia**[21]», porque hoy, la mayor amenaza que se cierne sobre los ordenadores es la de los programas maliciosos o «crimeware». Estos programas son desarrollados por ciberdelincuentes con el propósito de obtener dinero de forma ilegal.

El «**crimeware**» puede presentarse como virus, gusanos, troyanos u otro tipo de programas maliciosos. Lo que si está claro, es que en el período de alarmas y ataques en el que nos encontramos, se puede afirmar, que se inició en el 2009 y llega hasta la actualidad. Se trata de ataques en las Redes e ingeniería sociales, que es donde los ciberdelincuentes pueden hacerse con gran cantidad de datos personales. De ahí, el siguiente paso, es el ataque a dispositivos móviles[22], que son las plataformas más extendidas.

Según el **Ponemon Institute**[23], en sus estudios recientes y patrocinados por **HP Enterprise Security**[24], las cifras del estudio revelan que **el gasto anual medio en el que han incurrido las organizaciones estadounidenses ha sido de 8,9 millones de dólares**. Esto representa un aumento del 6% sobre el coste reportado en 2011, y un aumento del 38% respecto a 2010. Además, los resultados también revelan un aumento del 42% en el número de ataques cibernéticos, con las organizaciones experimentando un promedio de 102 ataques exitosos por año en comparación a los 72 ataques por año sufridos en 2011 y los 50 ataques anuales de 2010.

Gráficamente:



[21] GUTIÉRREZ FRANCÉS, María Luz. «Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley Penal en el espacio virtual)», en Redur 3, págs. 69-92. 2005.

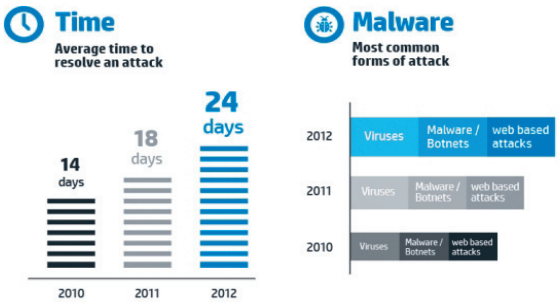
[22] CARACCIOLO, Claudio; SALLIS, Ezequiel. «*Los dispositivos móviles adorados por los consumidores llevan a profundas fallos de seguridad que hasta ahora están siendo descubiertas y tratadas*».http://www.root-secure.com/arch/Seguridad%20en%20Dispositivos%20Moviles%20Smartphone%20y%20Pocket%20PC.pdf

[23] http://www.ponemon.org/index.php

[24] http://www.hpenterprisesecurity.com/

Los ciberataques que más costes acarrean a las compañías siguen siendo los causados por códigos maliciosos, denegaciones de servicio, dispositivos robados o comprometidos y abusos malintencionados. Combinados, representan más del 78% de los costes por ciberdelitos que sufre una organización.

Gráficamente:



Por tanto, los ciberdelincuentes utilizan malware[25], bots[26], así como otros tipos de amenazas cada vez más sofisticadas, para atacar a las empresas y a las personas con acceso directo a internet, con muy diversas finalidades. Las intenciones que se esconden detrás de estos ataques pueden ser desde las ganancias económicas o la interrupción de las operaciones de negocio, hasta el robo de datos o incluso ataques tras los que existen motivaciones políticas.

En cualquier caso, estos ataques generan millones de euros de pérdidas cada año a las empresas, pero también sustracción de cantidades o datos importantes a nivel de persona física. También es verdad, que en el caso concreto de la empresa española, la mitad de los negocios, no tienen presupuesto suficiente para combatir este fenómeno[27].

Pero todo esto, ¿cómo afecta a las redes sociales[28]?

Pues bien, podemos definir la situación como aquella que se está desarrollando con preocupación y en crecimiento, dado que

[25] FUENTES, Luis Fernando. «*Malware, una amenaza de Internet*», en Revista Digital Universitario, v. 9, n.º 4, 2008, págs. 1-9.

[26] Un «*bot*» es un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado

[27] El 57 por ciento de los negocios españoles tienen problemas para conseguir más inversión para combatir el cibercrimen, según revela un estudio sobre riesgos de seguridad informática, llevado a cabo por B2B International y Kaspersky Lab.

[28] Redes sociales: como facebook, twitter, tuenti o Google Plus.

los distintos expertos coinciden en que **las redes sociales están siendo el punto de mira de los ciberdelincuentes**[29] y sobre todo, desde plataformas que cada vez muestran más interés a la población: Windows móbile, android, symbiam a través de los ya conocidos smartphones o teléfonos móviles, iPhones, iPads, etc (con los que navegamos y realizamos toda serie de gestiones personales, porque son como mini ordenadores), y son ciertamente vulnerables, al sufrir suplantaciones de identidad y toda serie de fraudes informáticos.

En este sentido, cada vez existe una mayor atracción por Facebook, twiter y como no, el conocido modo de chateo por medio de WhatsApp, en el que hemos encontrado estas formas de riesgo. Concretamente respecto de este último sistema de mensajería, nos vemos afectados en la privacidad de las comunicaciones, dado que para enviar mensajes, este servicio no pide un nombre de usuario y contraseña, sino que utiliza el propio número del teléfono y una clave que genera en función del móvil. Esto tiene el inconveniente de que cualquier persona puede enviar mensajes desde cualquier móvil que caiga en sus manos si éste no está protegido (p. ej.: está encendido y no pide clave o patrón de acceso o está apagado y no tiene PIN).

Es por ello, que la Oficina de Seguridad del Internauta[30] (OSI) del Instituto Nacional de Tecnologías de la Comunicación[31] (INTECO), publica en su blog una serie de consejos para evitar las **estafas en las redes sociales**[32], página a la que nos remitimos sin ánimo de extendernos en un asunto que a nivel personal, ya depende de cada uno, y que supone seguir las recomendaciones de los expertos. Por nuestra parte, nos interesa una vez introducidos y dado a conocer la fenomenología que nos afecta, es tratar la problemática y abordar su tratamiento desde un ámbito jurisprudencial y penal.

[29] Según el Instituto nacional de Tecnología de la Información. Agosto de 2012.

[30] https://www.osi.es/

[31] http://www.inteco.es/

[32] Estafas en las Redes Sociales: http://www.osi.es/es/actualidad/blog/2012/08/29/atento-las-estafas-que-circulan-por-las-redes-sociales; Para ver la extensión de las redes, proponemos un pdf: «Observatorio de las Redes Sociales 2012» y que se encuentra en la dirección:

http://www.google.es/url?sa=t&rct=j&q=informe%20resultados%20observatorio%20redes%20sociales&source=web&cd=5&ved=0CD4QFjAE&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2FNvISmny0o8OeyRTFYq8MuQ&ei=sI48UL7hJ4Gp0QWzoIH4Bw&usg=AFQjCNE5LyCyI6rM0MiS5g6v8k6FLdBn9g&cad=r

III. METODOLOGÍA JURÍDICA PENAL PARA HACER FRENTE AL CRECIMIENTO DEL CIBERDELITO. ESPECIAL ENFASIS DE ATAQUES CIBERNÉTICOS DURANTE LA CRISIS ECONÓMICA

Ya lo decían diversos medios de comunicación, entre ellos RTVE, que el ciberdelito[33] aumentaría durante la crisis económica. Y es más, se consideran infravalorados sus efectos, siendo curioso este hecho, si atendemos que cada día aparecen más de 70.000 nuevas muestras de software malicioso.

Para establecer de manera coherente unas estrategias tanto policiales, informáticas como legales, es preciso preguntarse ¿Ante quién o que nos enfrentamos? Nuestra prevención, se extiende más allá de las propias recomendaciones que a nivel de usuario nos corresponde garantizar.

En realidad quién ataca ya no es una persona concreta a la que podamos localizar en un ordenador. Lo difícil de rastrear del ciberdelincuente, es que actúa desde el anonimato, enmascarado a través de un software: virus o programa malicioso: malware[34], que será quién produzca los efectos deseados por su creador y que se ve favorecido por poder actuar a través de cualquier parte del mundo a través de cualquier medio conectado a internet, que estudia las distintas vulnerabilidades (bug 's) de los sistemas informáticos para tras descubiertas las mismas, producir un ataque.

Tradicionalmente, muchas de las características mencionadas, han respondido a lo que conocemos como hackers, pero en realidad cualquiera con conocimientos de informática y movido por el ansia del dinero, puede prestar su ciencia a empresas de seguridad o emplearla, para beneficio propio. Lo también preocupante, es que el perfil de estos **Black hats**[35] (hackers de sombrero negro),

[33] La primera sentencia por un «*ciberdelito*» de pedofilia en internet, que entendemos es una acción muy grave, fue por inaugurada por la Audiencia condena a tres años a un español que distribuía pornografía a nivel internacional http://www.belt.es/noticias/2003/diciembre/5/primera.htm

[34] WILLEMS, Eddy. «*La forma principal de evitar el malware es educar al usuario*». Oct ubre de 2011. http://www.ventasdeseguridad.com/201110186266/noticias/seguridad-informatica/eddy-willems-experto-en-seguridad-la-forma-principal-de-evitar-el-malware-es-educar-al-usuario.html

[35] Hackers de sombrero negro: Se le llama hacker de sombrero negro a aquel que penetra la seguridad de sistemas para obtener una ganancia personal o simplemente por malicia. La clasificación proviene de la identificación de villanos en las películas antiguas del vejo oeste, que usaban típicamente sombreros negros; Hackers de sombrero blanco: Se le llama hacker de sombrero blanco a aquel que penetra la

que yo denomino «**genios negros**», responde cada vez más, a jóvenes, en muchos casos menores de edad, lo que en este último caso aún perjudica el contraataque, porque la responsabilidad penal de los menores (en el caso de España), se exige a las personas mayores de catorce años y menores de dieciocho por la comisión de hechos tipificados como delitos o faltas en el Código Penal o en las leyes penales especiales. ¿Pero que ocurre cuando son menores de las edades indicadas y la gravedad de los ciberdelitos atenta seriamente a la sociedad?

Las redes son cada vez más convergentes y prestan mayores servicios, pero también aumentan su vulnerabilidad, por lo que se hace imprescindible el desarrollo de una correcta política de seguridad en la Red. Es necesario, por tanto, concienciar al legislador de la importancia de regular unos códigos penales que permitan tratar estos fenómenos con la actualidad que se merecen.

Es evidente que la tecnología se ha desarrollado a unos pasos mucho más agigantados que los sistemas legislativos pueden contemplar, que han obligado a los países ha tener que cambiar rápidamente la mentalidad frente a la aparición de las nuevas tecnologías y esto ha provocado, que se imponga la digitalización y la informatización, en todos los sectores.

Evidentemente, lo que beneficia a estos tipos de delincuentes, es que la informática no esté plenamente controlada por los Estados. Si a esto le añadimos, que en la época de crisis que atravesamos, se están viendo recortes que afectan a todos los sectores, no lo es menos en el área de la seguridad de los sistemas informáticos. La verdad es que sin ánimo de causar alarmismos innecesarios, defendemos que una central nuclear, puede estar menos protegida que un ordenador doméstico, aunque el riesgo de que se introduzca un virus en el ordenador que controla el núcleo principal de la central, como se puede uno imaginar, es bastante más alarmante, por las consecuencias que ello conlleva.

seguridad de sistemas para encontrar puntos vulnerables. La clasificación proviene de la identificación de héroes en las películas antiguas del viejo oeste, que usaban típicamente sombreros blancos; Hackers de sombrero gris: Como el nombre sugiere, se le llama hacker de sombrero gris a aquel que es una combinación de sombrero blanco con sombrero negro, dicho en otras palabras: que tiene ética ambigua. Pudiera tratarse de individuos que buscan vulnerabilidades en sistemas y redes, con el fin de luego ofrecer sus servicios para repararlas bajo contrato; Script kiddies: Se les denomina script kiddies a los hackers que usan programas escritos por otros para lograr acceder a redes de computadoras, y que tienen muy poco conocimiento sobre lo que está pasando internamente.

Sólo hay que navegar por internet y observar las noticias que se van generando, para comprender el alcance de las mismas[36]:

- Publican en Internet las contraseñas de más de 55.000 cuentas de Twitter.
- Un grupo de 'hackers' ataca los servidores de la NASA y de la ESA.
- El 'spam' llegga a Pinterest en forma de cupones.
- El FBI advierte de que 300.000 ordenadorres pueden quedarse sin internet en julio.
- Ramsoniock, un nuevo virus en Windows que bloquea el ordenador y pide un rescate.

Pero en este período global de recesión económica, no sólo la seguridad se ve afectada, sino que proliferan los fraudes precisamente entre quienes buscan ofertas de trabajo. En este sentido, basta con un e-mail de un remitente desconocido que ofrece una oferta laboral sin precedentes, prometiendo un gran sueldo, aunque el objetivo es conseguir que los que caigan en el engaño, realicen transferencias bancarias con las que blanquear dinero. A esta nuevo modus operandi, se le denomina «**Scammers**».

Esta situación ha supuesto un incremento en la cantidad de otros tipos de malware[37], como el **adware**[38], que en circunstancias normales serían secundarios con respecto a los troyanos bancarios.

Por ejemplo, se ha observado un incremento importante en el número de **estafas con falsos programas antivirus** que engañan a los usuarios para que realicen compras online de estos productos, en lugar de ataques de phishing para robar datos bancarios.

Estos son algunos de los datos clave descubiertos por **PandaLabs**[39]:

— De media, el mercado de valores norteamericano sufrió una caída del 3 al 7 por ciento entre el 1 de septiembre y el 9 de octu-

[36] PandaLabs, el laboratorio de análisis y detección de malware de Panda Security, ha emitido una alerta de seguridad que revela una relación directa entre la reciente volatilidad del mercado bursátil y el aumento en la aparición de nuevas amenazas.

[37] FUENTES, Luis Fernando. «*Malware, una amenaza de Internet*», en Revista Digital Universitaria, v. 9, n.º 4, 2008, págs. 1-9.

[38] Es un programa que consigue introducir información de publicidad web en nuestro ordenador, tras navegar por la red o descargar un programa. Se ejecuta automáticamente.

[39] http://www.pandasecurity.com/spain/homeusers/security-info/pandalabs/

bre. Sin embargo, ocurrió todo lo contrario en el «mercado del malware»: creció de manera substancial mientras caía la bolsa.

— Entre el 5 y el 16 de septiembre, los índices Dow Jones, ASDAQ, S&P 500 y Composite cayeron desde un porcentaje del 0.0 a un porcentaje negativo de -3.0 e incluso inferior. En ese mismo período el IBEX 35 español y el FTSE 100 londinense sufrieron también una importante caída. Sin embargo, durante ese mismo período de tiempo se produjo un aumento significativo en el número de amenazas diarias; por ejemplo, del 8 al 10 de septiembre, el volumen de amenazas diarias creció de 10.150 a más de 24.000.

— Del 14 al 16 de septiembre, los mercados de valores cayeron desde un porcentaje de -0.5 a -5.5 mientras que las amenazas diarias aumentaban en un 50 por ciento cada día, de 8.276 el día 14 a más de 31.404 el día 16.

En Rusia se ofrece abiertamente la venta de **Botnets**[40] o su alquiler, de manera que cuando se ejecuta una acción coordinada desde diversos ordenadores situados en diferentes partes del mundo, puede suponer un ataque informático a gran escala de envío masivo de publicidad no deseada o basura (spam) o cualquier otra acción con graves perjuicios económicos, siendo Android una plataforma móvil muy vulnerable.

Lo que se deduce de estos peligros, es por una parte, un negocio en crecimiento muy bien remunerado y un perjuicio para quienes lo sufren, dada la dispersión geográfica de los ordenadores que componen el ataque, es casi imposible encontrar un patrón de las máquinas que te están atacando y dado el alto número de ellas que lo estarán haciendo simultáneamente, no se puede evitar, porque no existe una solución real que funcione con efectividad.

Otros **modi operandi**[41], como novedades de este periodo, son:

— **Citas online fraudulentas:** igual que el virus «I Love You», las citas online fraudulentas tocan la fibra sensible de las víctimas para acometer su propósito. La típica estafa online de citas comienza cuando el estafador publica una foto atractiva en un sitio de citas en Internet. A continuación, el estafador envía mensajes a otros miembros del sitio web expresando su interés. El siguiente paso es

[40] Botnet es un término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática, para controlar todos los ordenadores y servidores, que infectados de forma remota enviando spam (correo basura) y que se venden normalmente a los spammers.

[41] Informe de Mcafee. Una gran década para el cibercrimen.

iniciar una conversación personal con las víctimas, normalmente a través del correo electrónico o mensajes instantáneos, en los que los ciberdelincuentes cuentan una triste historia, creando una relación personal para pedir dinero, bienes u otros favores.

— **Fraude nigeriano**[42]: Este timo, también conocido como el «fraude de pago por adelantado», por lo general consiste en un mensaje de correo electrónico no deseado de un extranjero que necesita ayuda para retirar millones de dólares de su país y ofrece al destinatario un porcentaje de su fortuna por ayudarle en la transferencia. Por desgracia, a pesar de que este timo es demasiado bueno para ser verdad, muchos de los destinatarios han picado y han perdido varios miles de dólares en el proceso, porque los ciberdelincuentes solicitan varios pagos por adelantado para facilitar el trato.

Ahora bien, para establecer una metodología que nos permita combatir los fenómenos estudiados, pasa por conocer nuestro sistema punitivo. De hecho, el caso particular español, no ayuda precisamente en este combate, dado el «**Código Penal español en su Ley Orgánica 10/1995, de 23 de noviembre, no contempla ni define los delitos informáticos como tales**», debiendo acudir a otras normativas y definiciones. En la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, tampoco lo define expresamente, si bien se refiere dentro del 248.2 a las manipulaciones informáticas, dentro de la SECCIÓN I «**De las estafas**».

Existen otros artículos, bajo otros títulos y capítulos del CP, en base a los cuáles podríamos hablar de las consecuencias que produce el fenómeno del delito informático, pero que en ningún caso aparecen como pertenecientes a una clasificación de estos. Así, encontramos, artículos del CP: 197, 278, 189, 186, 205, 206, 208, 209, 211, 263, 234, 237, 238, 239, 255, 623, 256, 270, 273, 282, 390 y 395, bajo los que los tribunales atribuyen los delitos por actos informáticos.

Ni siquiera, en la reforma[43] que se pretende por el gobierno actual, se plantea un reforzamiento del código penal que trate el delito informático, como así se requiere, porque las modificaciones consisten en introducir un nuevo delito consistente en la «**difusión de**

[42] http://www.sitiosinseguros.com/Estafa-Nigerianas-419.html

[43] http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CF0QFjAF&url=http%3A%2F%2Fwww.poderjudicial.es%2Fstfls%2FSALA%2520DE%2520PRENSA%2FEN%2520PORTADA%2FResumen%2520Informe%2520sobre%2520la%2520reforma%2520C%25C3%25B3digo%2520Penal.pdf&ei=AgNBUY6JJo6L4gS1tIHABg&usg=AFQjCNHjwa6HH3YcQyP3DjjGi-TBGCXIAw&sig2=x5uzoKChVZvgImctLsaDHg&bvm=bv.43287494,d.bGE&cad=rja

mensajes a través de las redes sociales» que inciten a alteraciones de orden público. Estará castigado con entre 3 meses y 1 año de cárcel, aunque también podrá ser sancionado con multa. Incluso, se prevee que se castigarán la difusión de «**vídeos íntimos por la red y sin permiso**».

El nuevo delito no especificará los canales de difusión de esos mensajes de incitación a la violencia, pero incluirá Twitter[44], Facebook[45], WhatsApp[46] o cualquier otra red social o de comunicación en general. Ahora bien, ¿a los efectos de combatir estos fenómenos delictivos resulta eficaz esta reforma en la parta que nos afecta según nuestro estudio? Evidentemente no, porque quizás se eviten las calumnias o las enjurias, pero no las principales figuras delictivas.

Llegados a este punto, creemos que ya se entiende que sea precisa una coordinación de los distintos sistemas nacionales e internacionales, tanto policiales, penales, como judiciales, para que resulte efectiva, cualquier medida encaminada a frenar la escalada de delitos informáticos[47]. Sin esta estrecha colaboración, nuestra seguridad quedará en entredicho, porque cualquier análisis actual, sin las debidas garantías de cumplimiento por parte de los estados, solo facilitará más las actuaciones de estos nuevos ciberdelincuentes o cibercriminales, según los casos.

III.1. ¿Cuál sería el tratamiento jurídico penal[48] dada la dificultad para apreciar la autoría delictiva?

A. En la consecución probatoria es crucial el papel de las empresas de telecomunicaciones y servidoras de Internet (ISPs[49]) que deben colaborar con la Justicia rápida, leal y eficazmente y que deben tratar de compatibilizar el desarrollo de la legítima libertad de expresión, comercio, conocimientos y comunicación que potencia Internet a través de sus múltiples mecanismos y posibilidades, y en lo que se basa principalmente su negocio, con la exclusión de ellos, sin embargo, del mayor número de contenidos ilícitos posible.

[44] https://twitter.com/
[45] https://es-es.facebook.com/
[46] http://www.whatsapp.com/
[47] http://webdeinformacion.blogspot.com.es/2012/09/delitos-informaticos-esta-usted.html
[48] HERNÁNDEZ DÍAZ, L., «*Aproximación a un concepto de Derecho penal informático*», en De la Cuesta Arzamendi, J. L. (dir.) Derecho penal informático, Cizur Menor, Civitas, 2010, págs. 35 y ss., especialmente 42 y ss.
[49] proveedor de servicios de Internet

B. Los ataques a varias víctimas ubicadas en territorios diferentes[50], su perpetración implica un delito masa, pudiéndose acumular delitos de acuerdo al 300[51] de la LECrim y para ser enjuiciados en una única causa que permita varias cosas:

— Evitar la desaparición de pruebas a que la investigación de un hecho atomizado suele llevar.

— Aplicar las agravaciones genéricas, principalmente la aplicación del delito continuado del artículo 74 del CP[52] (las múltiples diferentes estafas por importes a veces inferiores a los 400 euros de las estafas telefónicas o del phishing[53]).

— Posibilitar agravaciones específicas de estafa de especial gravedad en atención al valor de la defraudación del art. 250.6 CP, actuación en pornografía infantil perteneciendo a asociación o agrupación delictiva del artículo 189.3 e) del CP.

— Por otro, un correcto conocimiento de la dinámica comisiva del delito informático, que sólo se aprecia cuando aparece su reiteración sobre múltiples víctimas con un modus operandi delincuencial semejante que, entre otros extremos, nos permita confirmar que nos hallamos ante una actuación en grupo (una fuga de propiedad intelectual o industrial a favor de empresa de la competencia, o un intercambio organizado de pornografía infantil[54]).

[50] VELASCO NÚÑEZ, Eloy. «*Delitos cometidos a través de internet*», edición n.º 1, Editorial LA LEY, Madrid, Junio 2010.

[51] http://noticias.juridicas.com/base_datos/Penal/lecr.l2t4.html#a300

[52] La especificación del delito continuado, decía la Sentencia de 4 de julio de 1991 del Tribunal Supremo, requiere la concurrencia de una serie de requisitos: a) Pluralidad de hechos, ontológicamente diferenciables, que no hayan sido sometidos al enjuiciamiento y sanción por parte del órgano judicial, pendientes pues de resolver en el mismo proceso. b) Dolo unitario, no renovado, con un planteamiento único que implica la unidad de resolución y de propósito criminal. Se trata de un dolo global o de conjunto como consecuencia de la unidad de designio. Requiere, en definitiva, como una especie de culpabilidad homogénea, una trama preparada con carácter previo, programada para la realización de varios hechos delictivos, aunque puedan dejarse los detalles concretos de su realización para precisarlos después, conforme surja la oportunidad de ejecutarlos, siempre sin embargo con la existencia de elementos comunes que pongan de manifiesto la realidad de esa ideación global. Es, en suma, el elemento básico y fundamental del delito del artículo 69 bis.

[53] http://www.fraudwatchinternational.com/phishing/

[54] El Consejo de Europa ha definido la pornografía infantil como «cualquier material audiovisual que utiliza niños en un contexto sexual». Nuestra jurisprudencia en STS. 20.10.2003, consideró que la imagen de un desnudo -sea menor o adulto, varón o mujer- no puede ser considerada objetivamente material pornográfico, con independencia del uso que de las fotografías pueda posteriormente hacerse y, en la STS 10.10.2000 precisa que la Ley penal no nos ofrece una definición de lo que considera pornografía, refiriéndose a ella en los artículos 186 y 189 del Código penal.

C. Lo anterior, además, evita ciertos plazos cortos de prescripción en delitos usualmente castigados con baja pena (en torno a los tres años de privación de libertad máxima), y resuelve el a veces grave problema de la competencia dentro de la conexidad delictiva[55] a favor del que primero conociere del asunto[56], sin romper la continencia y unidad de la causa.

D. Al tratarse de delitos en que se conoce su dinámica comisiva[57], pero no su concreta vía de producción, y menos su autoría definitiva real, ante la cantidad de técnicas de anonimato que el delincuente puede y suele usar, la prueba de los mismos se reduce a la exclusiva búsqueda y hallazgo de los rastros y pistas técnicas que ha podido dejar el ataque en el sistema usado para delinquir, lo que por un lado obliga a asegurarlos para evitar su pérdida o desaparición, y por otro a una continua y escalonada cadena intermedia de injerencias en derechos fundamentales ajenos[58] (a la intimidad, a la cesión de datos y al secreto de las telecomunicaciones) para el avance de la investigación que, como pocos, hace básica y obligada la constante participación del juez instructor en su faceta de juez de garantías.

E. Lo anterior conlleva a una no deseada lentitud en la consecución de resultados y a una complementaria y por tanto costosa dependencia de la prueba pericial técnica[59] y sus necesidades intermedias (pantallazos, volcados de disco duro, análisis de los archivos, confección de la pericia en sí misma, etc.), que a veces explica por qué se denuncia menos este tipo de delitos y su también menor eficacia, resumida en el aserto certísimo de que obliga a investigaciones muy complejas, caras e intrusivas, para ser finalmente castigados con poca pena.

F. Por encima de todo lo anterior, si hay alguna característica singular de la delincuencia informática, más que la de su sofisticación tecnológica, es la de que el infractor suele ser un delincuente cobarde, que «**tira la piedra y esconde la mano**», actuando casi sin riesgo y a distancia, utilizando bien técnicas humanas de anonimato mediante las correspondientes suplantaciones de la personalidad,

[55] Artículo 17 LECrim.

[56] Artículo 18.2 LECrim.

[57] http://mural.uv.es/procesales/delitos/Da%F1os.pdf

[58] BAÑULS GÓMEZ, Francisco Alexis. «*Las intervenciones telefónicas a la luz de la jurisprudencia más reciente*». Noticias Jurídicas. 2007. http://noticias.juridicas.com/articulos/55-Derecho%20Penal/200702-981932563274752514.html

[59] Informar y concienciar a los juristas de los avances en materia probatoria en los casos en que intervenga el factor informático en el proceso, así como de los importantes beneficios de la incorporación y uso de las nuevas tecnologías en el propio proceso judicial.

uso de nicks o apodos, delinquiendo desde cibercafés, ciberuniversidades[60], blogs, foros, chats, etc., o técnicas propiamente dichas que la informática enseña y que prácticamente hacen anónima su utilización, como pueden ser los proxys[61], anonimizadores web, servidores de correo web, remailers[62], dialers[63], o técnicas de por sí delictivas como cierto tipo de malware, como los keyloggers[64].

La determinación de la autoría concreta del real infractor en los supuestos del uso de técnicas de ingeniería social o informática anonimizadoras[65] y, en su caso, en los supuestos de uso compartido del ordenador, no es diferente en las investigaciones por delitos informáticos que en las de delitos tradicionales, pudiendo utilizarse cualesquiera medios de prueba legalmente admitidos, empezando por los que aporta la propia técnica como instrumento al servicio de la investigación procesal misma.

Y si no fuese posible mediante la oportuna prueba técnica pericial para la detección de las señas IP del usuario o el rastreo de las cuentas bancarias asociadas o por la documental, y el conocimiento de la clave de usuario y contraseña de cada cual pudiese ser conocida por terceros, cabe la determinación de la convicción judicial por la testifical (uso del ordenador por el inculpado en exclusiva, utilización de apodos, seudónimos o nicks[66], descartes de la coartada indicada por el imputado, testimonio condicionado del co-imputado[67], etc.), confesión del inculpado[68] e incluso por determinación indiciaria siempre que convincentemente se razone (v. gr., analizando a quién le llega el dinero, quién tiene un móvil espurio, a quién le be-

[60] http://www.abc.com.py/articulos/ciberuniversidades-7079.html

[61] ¿Qué es un proxy-caché (o alterno)? http://portal.uned.es/portal/page?_pageid=93,581860,93_20540461&_dad=portal&_schema=PORTAL

[62] Es un servidor que recibe emails en un formato especial, los procesa eliminando las cabeceras, y los dirige hasta el destinatario del mensaje.

[63] Son programas maliciosos, o código maligno escondido en webs, que hace que nuestro módem marque a un sitio web de pago.

[64] Como un programa diseñado para, en secreto, monitorear y registrar cada pulsación, pudiendo obtener claves o datos vitales para el acceso a un ordenador, red o cuenta bancaria, entre otros tipos de actuaciones, sin el consentimiento del autor.

[65] http://campusvirtual.unex.es/cala/epistemowikia/index.php?title=Anonimizadores_-_Proxies_an%C3%B3nimos_-_Anti-censura

[66] OLIVEROS, Francisco. «*La importancia de un Nick en internet*». http://blogandweb.com/web-20/la-importancia-de-un-nick-en-internet/

[67] SÁNCHEZ GARCÍA DE PAZ, Isabel. «*El coimputado que colabora con la justicia penal*». Revista Electrónica de Ciencia Penal y Criminología. http://criminet.ugr.es/recpc/07/recpc07-05.pdf

[68] URIARTE VALIENTE, Luis M. «*El proceso penal español: jurisprudencia sistematizada*». Ed. La ley. Madrid, 2007. pág. 716.

neficia, los conocimientos informáticos del inculpado[69], demostrando la mentira de la declaración del imputado[70], probando que no es posible la infiltración en el uso del ordenador por terceras personas, no dando el acusado explicación satisfactoria de la posesión[71], etc.).

G. En la consecución probatoria es crucial el papel de las empresas de telecomunicaciones y servidoras de Internet (**prestadores de servicio y proveedores de Internet**), que deben colaborar con la Justicia rápida, leal y eficazmente y que deben tratar de compatibilizar el desarrollo de la legítima libertad de expresión, comercio, conocimientos y comunicación que potencia Internet a través de sus múltiples mecanismos y posibilidades, y en lo que se basa principalmente su negocio, con la exclusión de ellos, sin embargo, del mayor número de contenidos ilícitos posible.

Como las empresas dedicadas a la introducción de contenidos en Internet no los pueden controlar (pues meramente juegan el papel técnico de ser intermediarios de la circulación de información), y sería exacerbado imponerles su vigilancia, se les ha exigido (art. 11 de la Ley 34/2002, de 11 de julio) un carácter de custodia pasiva, de modo y manera que responderán penalmente, en su caso, no por no haber detectado en sus páginas la existencia de contenidos ilícitos, sino si una vez hecho, notificado, ordenado o sabido, éstos no los retiran (comisión por omisión[72]), además de en los supuestos en que ellos sean los propios creadores directos o cooperadores necesarios[73] en la difusión del contenido ilícito o asuman el papel de moderadores o gestores responsables, por ejemplo de foros de debate.

No le son de aplicación, en consecuencia, los criterios de autoría en cascada establecidos en el art. 30 CP para los delitos de difusión mecá-

[69] Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen.

[70] En este sentido, las SSTC 129/1996 y 153/1997, en base a los artículos 17.3 y 24.2 de la CE y artículo 520.2 a) y b) de la LECrim. recuerdan que el imputado no tiene obligación de decir la verdad, sino que puede callar total o parcialmente, o incluso mentir, en virtud de sus derechos a no declarar contra sí mismo, a no confesarse culpable y a no contestar a alguna o algunas de las preguntas que se le formulen.

[71] SAP Madrid Sección 2.ª de 6/05/2004.

[72] «*La comisión por omisión*». http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CGUQFjAE&url=http%3A%2F%2Fwww.unav.es%2Focw%2Fdpenal2%2Fpdf%2Fn63.pdf&ei=YxtBUc6fN4OChQeQroGgBg&usg=AFQjCNGv8T2gxHRU9-wGAjvEs6td17Giuw&sig2=1aboodVGGZlYFARuxdMuoA&bvm=bv.43287494,d.ZG4&cad=rja

[73] ESTRELLA GUTIÉRREZ, David. «*La responsabilidad en cascada en el medio digital: insuficiencia del art. 30 del CP. 1995*». Noticias jcas. Marzo de 2002. http://noticias.juridicas.com/articulos/20-Derecho%20Informatico/200203-275591221022700.html

nica[74], pues amén de parecer pensados para la prensa, son más delitos, los informáticos, de difusión telemática y, en cualquier caso, la capacidad de control sobre la introducción de contenidos presuntamente ilícitos en el proveedor es inexistente.

Vulneraría el principio de culpabilidad[75] hacer recaer responsabilidad penal en los prestadores de servicio y proveedores de Internet[76], pues ellos no originan, ni modifican, ni seleccionan, ni destinan información de contenido ilícito en el hecho de acceder o transmitir la que hayan hecho sus usuarios, y no tienen sobre los mismos, mientras dure esta ignorancia, ningún poder de dirección, autoridad o control.

H. Por otra parte, como lo ilícito fuera de la Red, continúa siéndolo también al cometerse en la Red, pero quizá su difusión y expansión universal añadan un plus de gravedad en cuanto a la posibilidad de generar delitos-masa con multiplicidad de víctimas, y si a eso se añaden las técnicas de anonimato (proxys, servidores de correo web, anonimizadores web, cibercafés, cibercentros sin identificación de usuarios, teléfonos móvil GPRS con tarjetas prepago) que ayudan a dejar impunes muchas de estas conductas, se entendería que el legislador cree una agravante genérica -por ejemplo, la de colgar en la red la grabación de un delito con ánimo de difundirlo aunque no se haya participado en él, castigando una especie de colaboración omisiva en el mismo- o algunas específicas para los delitos convencionales cometidos a través de Internet, o que la pena concreta que los jueces impongan en los delitos en estas circunstancias se alejen de los mínimos estándar, por la profesionalidad delictiva que desprenden.

I. Además, la generalización y el uso cotidiano (por accesible y barato) de ciertas innovaciones tecnológicas, ha obligado a la luz de las mismas a interpretar y reinterpretar la protección de ciertos

[74] Supuestos especiales: Autoría de delitos cometidos a través de la imprenta; autoría de las faltas. http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDsQFjAB&url=http%3A%2F%2Fwww.unav.es%2Fpenal%2Fdelictum%2Fn126.pdf&ei=-wtBUejhMe3Y7Ab9t4GgDg&usg=AFQjCNF1BGqn6PKfWz92ZMyodksWwZQQGQ&sig2=uRW7C9q-tmeqYB9lZ7I3uw&bvm=bv.43287494,d.ZGU&cad=rja

[75] El principio de culpabilidad, como garantía individual, se halla dentro del conjunto de postulados esenciales a todo Estado Constitucional de Derecho.

[76] MORALES GARCÍA, Oscar. «*Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información*». Marzo de 2001. http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDQQFjAA&url=http%3A%2F%2Fwww.uoc.edu%2Fojs%2Findex.php%2Fin3-working-paper-series%2Farticle%2Fdownload%2Fn1-morales%2F336&ei=HRxBUeTXGYOHhQfB94CgBg&usg=AFQjCNGHhN5Day-zdY78rXcL6lV7EdwMBw&sig2=bHNf-Gm9cZsIbufSmjiqtAA&bvm=bv.43287494,d.ZG4&cad=rja

derechos fundamentales (la intimidad, la propia imagen, el secreto de las telecomunicaciones, la intimidad informática, la protección de los datos tratados automatizadamente[77], la privacidad y las libertades de expresión e información) que, sin embargo, son prioritarios y preexistentes.

J. En España todavía la delincuencia informática encuentra espacios de impunidad, que se suman a la posible ineficacia de medios policiales y judiciales, un escaso despliegue normativo de instrumentos que no se entiende por qué no se desarrollan, como es el hecho paradigmático de no haber ratificado España el Convenio del Cibercrimen del Consejo de Europa[78], o no haber desarrollado reglamentariamente la **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información**[79], y la posterior **Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información**[80], creando, por ejemplo, procedimientos monitorios para la retirada de contenidos nocivos y/o delictivos sin autor de Internet, tanto para los supuestos de simple denuncia como para aquellos en que por haber oposición, necesariamente hayan de dirimirse en algún procedimiento judicial acelerado en la vía penal o en la contenciosa, o, yendo más allá, complementando el actual Código Penal, contemplando como delitos realidades ahora atípicas (la suplantación informática e inconsentida de personalidades ajenas, el acoso informático[81] que bloquee o empeore el normal uso de la informática y sus comunicaciones, etc.) o modalidades complejas como el phishing, la denegación de servicio (DDoS) o el sabotaje informático, para reducir sus nada desdeñables problemas concursales.

[77] Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108). http://www.coe.int/t/dghl/standardsetting/dataprotection/global_standard/D%C3%A9pliant%20Conv108_es.pdf

[78] España ratificó el 3 de junio de 2010, el Convenio sobre «cibercrimen» del Consejo de Europa, el primer tratado internacional sobre infracciones penales cometidas en Internet, según informó hoy esta organización paneuropea. El texto del Convenio, que entrará en vigor en España el próximo 1 de octubre, protege los derechos de autor y lucha contra la pornografía infantil.

[79] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. http://noticias.juridicas.com/base_datos/Admin/l34-2002.html. Ver también, GIMENO, M. (dir.), «*eEspaña, Informe anual sobre el desarrollo de la sociedad de la información en España, Fundación Orange*». Internet, en http://www.informeeespana.es/ docs/eE2011.pdf (última visita el 11 de junio de 2012).

[80] http://www.boe.es/buscar/doc.php?id=BOE-A-2007-22440

[81] Acoso en redes sociales. http://www.delitosinformaticos.com/09/2012/delitos/como-actuar-ante-un-acoso-en-redes-sociales#.UUEdfNnxfZk

K. Dado el aumento en crecimiento de los ataques, se hace preciso que las medidas procesales penales, se vean fortalecidas por diligencias que se realicen en sedes no judiciales y que buscan la prevención en la averiguación del delito, que no solo implica a la policía, sino también, de manera muy destacada, a los ciudadanos. La prevención[82] consiste en: asegurar la escena, identificar los elementos de convicción relacionados con la acción delictiva, capturar la información, preservar las fuentes de prueba y rastros hallados y dejarlos debidamente custodiados para su posterior análisis.

En el aseguramiento de la escena del delito tecnológico[83], entre otros, se deberá analizar qué elementos están relacionados con la infracción para descartar los ajenos y descubrir qué puede saber su presunto autor, verificando la mejor manera para conservar los rastros delictivos según las peculiaridades que presente lo encontrado (no apagado de pantallas encendidas hasta asegurar lo almacenado en los log, congelar la memora RAM con nitrógeno líquido para descubrir la contraseña de usuario, tirar del cable para no borrar, etc.).

La captura de la información pertinente seleccionada se realiza mediante el copiado, clonado o volcado in situ de los discos duros (para evitar formateos, enmascaramientos o borrados posteriores y para asegurar el conocimiento de las señas IP del último atacante y la actividad pasada recogida en los proxies y en las copias de seguridad).

L. Actualmente las renovadas posibilidades de la Web 2.0[84], que hacen del internauta un protagonista cada vez más activo e influyente en la creación de contenidos de todo tipo. Pero esto, quizás sean las causas de la existencia en crecimiento de las vulnerabilidades que hemos mencionado. La versión que releva a la 2.0 sería la 3.0 o Web inteligente, pero que para nuestros fines, quizás no sea tampoco apropiada. El estado actual, nos llevará hacia la creación una «**Web blindada**», exclusiva para proteger de manera efectiva las operaciones comerciales a nivel individual y empresarial, que permita la navegación segura, sin contenidos maliciosos y en el que exista un control de la seguridad sin bug's. Una web, en el que sólo tenga cabida la actividad de los mercados y de las empresas, administraciones, aeropuertos, energía, transportes, alimentación. De manera paralela,

[82] VELASCO NÚÑEZ, Eloy. «*Delitos cometidos a través de Internet. Cuestiones procesales*». Ed. La ley. 2010.

[83] FACCIOTI, Raúl; GONZÁLEZ, Omar. «*Abordaje tecnológico a la escena del crimen*». http://www.consultorespericiales.com/archivos/abordaje_tecnologico.pdf

[84] Artículo: «*Entienda la web 2.0 y sus principales servicios*». http://www.eduteka.org/Web20Intro.php

pero con acceso público, otra web dónde se permita los contenidos personales y el ocio. Todo esto, es hoy por hoy inconcebible.

4. CONCLUSIONES[85]

El robo de información[86] y la interrupción del negocio continúan representando los costes externos más altos. Sobre una base anual, este coste representa un 44% del total de los costes externos, frente al 4% de 2011. En cuanto a la interrupción del negocio o la pérdida de productividad, representa el 30% del total de los costes externos, frente al 1% de 2011.

La implementación de soluciones de Inteligencia avanzada permite mitigar el impacto de los ciberataques[87]. Las organizaciones que hacen uso de las soluciones SIEM (Gestión de Eventos e Información de Seguridad) ahorran casi 1,6 millones de dólares en costes. Como consecuencia, estas organizaciones experimentaron un coste considerablemente más bajo de recuperación, detección y contención que aquellas que no hacen uso de soluciones SIEM.

Los ciberataques pueden ser costosos si no se resuelven con rapidez. La media de tiempo para resolver un ciberataque es de 24 días, pero, de acuerdo al estudio, puede llegar a los 50 días. El coste medio en el que han incurrido las compañías durante este periodo de 24 días ha sido de 591.780 dólares, lo que representa un aumento del 42% sobre el coste medio estimado del pasado año, que se situaba en los 415.748 dólares durante un período de 18 días.

La recuperación y detección siguen siendo las actividades internas más costosas asociadas a los delitos cibernéticos. Sobre una base anual, este tipo de actividades representa casi la mitad de los costes internos totales, siendo los gastos de operaciones y trabajo los que se llevan la mayor parte.

La fragilidad de los sistemas informáticos favorece la actividad fraudulenta de las nuevas figuras delictivas, en tiempo de recortes económicos. Las compañías de seguridad o empresas internacionales, contratan a cualquier experto para que intente pe-

[85] HP ha presentado los datos de la tercera edición del «*Estudio sobre el cibercrimen 2012*».

[86] El robo de información es una de las peores amenazas para las organizaciones; y, sin embargo, los ejecutivos le han delegado este problema a terceros. El robo de información es el delito digital más frecuente en el sector turístico.

[87] Impacto financiero del Cibercrimen incrementa 40%. http://www.ponemon.org/

netrar en sus sistemas de seguridad a través de debilidades tecnológicas de su infraestructura y de ese modo, reforzar sus sistemas.

La empresa de seguridad Symantec, cuenta con 300 millones de clientes en el mundo y comercializa en España los sistemas de seguridad Norton 360, Norton Antivirus y Norton Internet Security. 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 este sentido, lo más relevante:

— Las pérdidas medias a nivel mundial por víctima son de 152 euros en costes financieros directos.

— En los últimos 12 meses, cerca de 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[88] 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.

[88] CLOUGH, J., «*Principles of Cybercrime*», Cambridge, Cambridge University Press, 2010, pág. 4.

Lo cierto, es que las conclusiones hablan por si solas, pero existe una distracción en los gobiernos, dado que las autoridades están concentradas en la economía, la lucha contra el crimen cibernético no es una prioridad en su agenda. La Escasez de policías cibernéticos, impide luchar efectivamente contra el crimen cibernético, por falta de capacitación dedicada y remuneración suficiente.

Existe una criminalidad oculta: Rusia y China se han convertido en puertos seguros para los criminales cibernéticos. Brasil es uno de los países de mayor crecimiento como «chivo expiatorio» para el crimen cibernético. Pero lo más grave de todos estos datos, es que la ciberdelincuencia[89] se está convirtiendo en estos momentos difíciles, en un negocio muy apetitoso para algunos, a costa de los demás.

Y lo más incomprensible a estas alturas, es que la aplicación de la ley está limitada por las fronteras físicas de los países, mientras que los criminales cibernéticos operan rápidamente más allá de las fronteras. La reforma que pretende nuestro gobierno del CP, no solo es insuficiente a efectos del combate contra el ciberdelito en sus múltiples facetas, sino que ni se acerca a la realidad actual que subyace en el entorno web y que afecta tanto a empresas como a los ciudadanos. Se hace preciso, una ruptura con el esquema web que tenemos definido. Es imposible controlar con la forma de navegación que existe actualmente, los ilícitos en el ciberespacio. No solo es preciso un cambio procesal sino de la forma de acceso a internet.

5. BIBLIOGRAFÍA

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. «*La defensa de la intimidad de los ciudadanos y la tecnología informática*». Editorial Aranzadi S.A., Pamplona, 1999.

BAÑULS GÓMEZ, Francisco Alexis. «*Las intervenciones telefónicas a la luz de la jurisprudencia más reciente*». Noticias Jurídicas. 2007. http://noticias.juridicas.com/articulos/55-Derecho%20Penal/200702-981932563274752514.html

CARACCIOLO, Claudio; SALLIS, Ezequiel. «*Los dispositivos móviles adorados por los consumidores llevan a profundas fallos de seguridad que hasta ahora están siendo descubiertas y tratadas*».http://www.root-secure.com/arch/Seguridad%20en%20Dispositivos%20Moviles%20Smartphone%20y%20Pocket%20PC.pdf

[89] GUTIÉRREZ FRANCÉS, María Luz. «*Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley Penal en el espacio virtual)*», en Redur 3, 2005, págs. 69-92.

CLOUGH, J. «*Principles of Cybercrime*», Cambridge, Cambridge University Press, 2010, pág. 4.

ESTRELLA GUTIÉRREZ, David. «*La responsabilidad en cascada en el medio digital: insuficiencia del art. 30 del CP. 1995*». Noticias jcas. Marzo de 2002. http://noticias.juridicas.com/articulos/20-Derecho%20Informatico/200203-275591221022700.html

FACCIOTI, Raúl; GONZÁLEZ, Omar. «Abordaje tecnológico a la escena del crimen». http://www.consultorespericiales.com/archivos/abordaje_tecnologico.pdf

FUENTES, Luis Fernando. «*Malware, una amenaza de Internet*», en Revista Digital Universitario, v. 9, n.º 4, 2008, págs. 1-9.

GUTIÉRREZ FRANCÉS, María Luz. «*En torno a los fraudes informáticos en el derecho español*», que conviene no confundir el fraude informático con el delito informático, esto es, la parte con el todo, puesto que aquél no es más que un tipo de delincuencia informática, en AIA, núm. 11, abril, 1994, pág. 7.

GUTIÉRREZ FRANCÉS, María Luz. «*Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley Penal en el espacio virtual)*», en Redur 3, 2005, págs. 69-92.

HERNÁNDEZ DÍAZ, L., «*Aproximación a un concepto de Derecho penal informático*», en De la Cuesta Arzamendi, J. L. Derecho penal informático, Cizur Menor, Civitas, 2010, págs. 35 y ss., especialmente 42 y ss.

JORDÁN, Javier y TORRES, R. Manuel. «*Internet y actividades terroristas: el caso del 11-M*», en El profesional de la información, v. 16, n. 2, marzo-abril, 2007, págs. 123-130.

LARKIN, Eric. «*Cibercrimen (I): Delincuentes profesionales online*», en PCWorld, n.º 224, 2005, págs. 26-30.

MORALES GARCÍA, Oscar. «*Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información*». Marzo de 2001. http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDQQFjAA&url=http%3A%2F%2Fwww.uoc.edu%2Fojs%2Findex.php%2Fin3-working-paper-series%2Farticle%2Fdownload%2Fn1-morales%2F336&ei=HRxBUeTXGYOHhQfB94CgBg&usg=AFQjCNGHhN5Day-zdY78rXcL6lV7EdwMBw&sig2=bHNfGm9cZsIbufSmjiqtAA&bvm=bv.43287494,d.ZG4&cad=rja

OLIVEROS, Francisco. «*La importancia de un Nick en internet*». http://blogandweb.com/web-20/la-importancia-de-un-nick-en-internet/

MAGLIONA MARKOVICH, Paul Claudio; LÓPEZ MEDEL, Macarena. «*Delincuencia y fraude informático*». Derecho comparado y Ley 19223. Ed. Jurídica de Chile. 1999.

MCAFEE: «*La recesión económica es un semillero para la actividad fraudulenta pues los delincuentes cibernéticos se aprovechan del clima de miedo y ansiedad que hay entre los consumidores*» *http://www.eluniversal.com.mx/articulos/51700.html*

ORTA MARTÍNEZ, Raymond. «*Ciberterrorismo*», en Revista de Derecho Informático, no. 082, mayo 2005.

PÉREZ GIL, Julio. «*El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito*». Ed. La Ley, Madrid 2012.

ROGRÍGUEZ BERNAL, Antonio. «*Los cibercrímenes en el espacio de libertad, seguridad y justicia*», en Revista de Derecho Informático, no. 103, febrero 2007, págs. 1-42.

ROMEO CASABONA, Carlos María. «*El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*». 1.ª ed., 1.ª imp. Septiembre 2006.

SÁNCHEZ GARCÍA DE PAZ, Isabel. «*El coimputado que colabora con la justicia penal*». Revista Electrónica de Ciencia Penal y Criminología. http://criminet.ugr.es/recpc/07/recpc07-05.pdf

SALGADO, Víctor. «*La crisis no sólo no frena el desarrollo de lo Sociedad de la Información sino que la acelera*». Entrevista: http://issuu.com/parnet-tic/docs/boletin_n19_final_120ppp

URIARTE VALIENTE, Luis M. «*El proceso penal español: jurisprudencia sistematizada*». Ed. La ley. Madrid, 2007. pág. 716.

VELASCO NÚÑEZ, Eloy. «*Delitos cometidos a través de internet*», edición n.º 1, Editorial LA LEY, Madrid, Junio 2010.

WILLEMS, Eddy. «*La forma principal de evitar el malware es educar al usuario*». Oct ubre de 2011. http://www.ventasdeseguridad.com/201110186266/noticias/seguridad-informatica/eddy-willems-experto-en-seguridad-la-forma-principal-de-evitar-el-malware-es-educar-al-usuario.html

LEY DE ENJUCIAMIENTO CRIMINAL

Artículo 17 LECrim.

Artículo 18.2 LECrim.

Artículo 282 LECrim

Artículos 544 bis y ter LECrim

Artículo 770.3 LECrim

520.2 a) y b) de la LECrim

SENTENCIAS

SAP Madrid Sección 2.ª de 6/05/2004.

SAP 17.ª Madrid 4/10/2006

STS 23/01/2007

STS. 20/10/2003

SSTC 129/1996 y 153/1997

SAP Madrid Sección 2.ª de 6/05/2004.

DIRECCIONES WEB

https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/normativa_estatal/common/pdfs/E.2-cp--C-oo-digo-Penal.pdf

http://campusvirtual.unex.es/cala/epistemowikia/index.php?title=Anonimizadores_-_Proxies_an%C3%B3nimos_-_Anticensura

http://www.osi.es/es/actualidad/blog/2012/08/29/atento-las-estafas-que-circulan-por-las-redes-sociales

http://www.fraudwatchinternational.com/phishing/

http://www.google.es/url?sa=t&rct=j&q=informe%20resultados%20observatorio%20redes%20sociales&source=web&cd=5&ved=0CD4QFjAE&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2FNvISmny0o8OeyRTFYq8MuQ&ei=sI48UL7hJ4Gp0QWzoIH4Bw&usg=AFQjCNE5LyCyI6rM0MiS5g6v8k6FLdBn9g&cad=rja

http://www.republica.com/2013/01/13/facebook-y-twitter-protagonizaron-la-mayoria-de-ataques-ciberneticos-de-2012_600061/

http://portal.uned.es/portal/page?_pageid=93,581860,93_20540461&_dad=portal&_schema=PORTAL

http://www.symantec.com/es/es/index.jsp

http://www.kaspersky.com/sp/

http://www8.hp.com/es/es/home.html

http://www.cisco.com/web/learning/netacad/index.html

http://www.microsoft.com/es-es/default.aspx

http://www.coe.int/t/dghl/standardsetting/dataprotection/global_standard/D%C3%A9pliant%20Conv108_es.pdf

http://www.eduteka.org/Web20Intro.php

http://www.belt.es/noticias/2003/diciembre/5/primera.htm

http://www.pandasecurity.com/spain/homeusers/security-info/pandalabs/

http://www.ponemon.org/index.php

http://noticias.juridicas.com/base_datos/Admin/l34-2002.html

https://www.osi.es/

http://www.informeeespana.es

http://www.inteco.es/

http://www.ponemon.org/

http://www.sitiosinseguros.com/Estafa-Nigerianas-419.html

https://twitter.com/

https://es-es.facebook.com/

http://www.boe.es/buscar/doc.php?id=BOE-A-2007-22440

http://www.whatsapp.com/

http://www.delitosinformaticos.com/09/2012/delitos/como-actuar-ante-un-acoso-en-redes-sociales#.UUEdfNnxfZk

http://webdeinformacion.blogspot.com.es/2012/09/delitos-informaticos-esta-usted.html

http://noticias.juridicas.com/base_datos/Penal/lecr.l2t4.html#a300

http://mural.uv.es/procesales/delitos/Da%F1os.pdf

http://campusvirtual.unex.es/cala/epistemowikia/index.php?title=Anonimizadores_-_Proxies_an%C3%B3nimos_-_Anti-censura

http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CGUQFjAE&url=http%3A%2F%2Fwww.unav.es%2Focw%2Fdpenal2%2Fpdf%2Fn63.pdf&ei=YxtBUc6fN4OChQeQroGgBg&usg=AFQjCNGv8T2gxHRU9-wGAjvEs6td17Giuw&sig2=1aboodVGGZlYFARuxdMuoA&bvm=bv.43287494,d.ZG4&cad=rja

http://www.boe.es/buscar/doc.php?id=BOE-A-2007-22440

Zaragoza, a 17 de marzo de 2013.