1ª JORNADA TIC SOBRE CIBERDELINCUENCIA

CIBERDELINCUENCIA INTRUSIVA: HACKING Y GROOMING.

I.- CIBERDELINCUENCIA INTRUSIVA.

Actualmente se viene incluyendo por la doctrina mayoritaria bajo el concepto de Delito informático tanto el delito tradicional cometido a través de ordenador o la Red (Internet) como el estrictamente entendido como tal, esto es el dirigido contra la informática, los datos y la información informatizada, o las redes de telecomunicación, especialmente a través de Internet, y se suele diferenciar una clasificación tripartita de los mismos. Así junto a la denominada *ciberdelincuencia económica*, que incluye los denominados delitos económico patrimoniales vinculados a la informática, y a los ataques por medios informáticos contra intereses supraindividuales, como el *ciberespionaje* y el *ciberterrorismo*, un gran tercer grupo denominado *ciberdelincuencia intrusiva*, configurado por aquellos ataques por medios informáticos contra la intimidad y la privacidad, concepto éste que incluye, más allá del anterior, todos los bienes protegidos en el art. 18 de la Constitución Española de 1978: el honor, la intimidad personal, la familiar, la propia imagen, el domicilio, el secreto de las comunicaciones o incluso el uso adecuado y correcto de la informática.

Configuran aproximadamente el 25% de los delitos objeto de denuncia y vienen actualmente recogidos en el Código Penal en:

- Amenazas informáticas (art. 169)
- Coacciones informáticas (art. 172)
- Distribución de material pornográfico entre menores de edad (art. 186)
- Pornografía infantil (art. 189)
- Descubrimiento y revelación de secretos en cuanto a la protección de datos personales (arts. 197 a 200)
- Injurias y Calumnias informáticas (art. 211)
- Cesión no consentida de datos ajenos (en la infidelidad en la custodia de documentos y violación de secretos: art. 417 y 418).

Es en el ámbito de los delitos de Descubrimiento y revelación de secretos (art. 197.3 nuevo CP., cambiando la numeración de los precedentes apartados 3, 4, 5 y 6) donde se introduce el nuevo delito informático intrusivo por excelencia, el Hacking o acceso ilegal, siendo que dicho Texto normativo únicamente ha modificado la redacción de las letras a) y b) del apartado 1 del

art. 189 relativo a la Pornografía infantil, y se han introducido otra novedad significativa entre los ilícitos penales, el *child grooming* o acoso infantil, que van a ser objeto de desarrollo en la presente ponencia, aunque sin desvalorar los otros tipos referidos que evidentemente tienen una enorme proyección de futuro al ser los autores conocidos personas jóvenes, que incluso no rehúyen la delincuencia organizada, evolucionan en el uso de la Tecnologías de la Informática y de la Comunicación (TIC), obligando a una continua actualización normativa y operativa de quienes los combaten, y crecen de forma desmesurada año por año, como la Pornografía infantil a través de Internet que se multiplicó por 4 en España entre 2004 y 2005.

II.- ANTECEDENTES.

El hecho de la práctica constatación de un cambio de paradigmas de la propia sociedad, en muchos ámbitos de las relaciones jurídicas y sociales acontecido por la introducción de las tecnologías de la información, y que cambiaron ya la sociedad del siglo XX, y sobre todo en el último decenio, incluso promoviéndose por la administración y organismos públicos una mayor facilidad en el acceso, búsqueda, intercambio y difusión de información contenida en redes y sistemas informáticos, constituyendo asimismo un aumento del riesgo de perpetración de actos ilícitos, la globalización del fenómeno, a tenor de la mayor potencia de los sistemas informáticos con mayores prestaciones y su generalizada disponibilidad para cualquier persona consolidándose en una "informática de masas", y su coincidencia en un nuevo espacio virtual, el ciberespacio, que llega a producir nuevas formas de realidad y en el que *"lo real puede convertirse en falso, el original, en copia y el ser, en identidad virtual"*, con independencia de un punto concreto del planeta, ha supuesto el configurar el delito informático como más móvil y más internacional, con una gran potencialidad como medio de anonimato e impunidad en las comunicaciones, incluso entre los delincuentes, y su utilización ha venido incluso siendo constatada en las organizaciones criminales.

Es por ello que ya en el marco de la UE, los dictámenes y comunicaciones elaborados sobre los delitos informáticos o sobre la protección de la infancia en Internet, se han expuesto los principios esenciales que respaldan la lucha contra el uso de Internet con fines delictivos o criminales, y en los que aún rechazando la censura, la vigilancia generalizada y los obstáculos a la libertad de expresión y comunicación en la red global se afirma categóricamente que “la red Internet no está al margen de la ley”.

Y así se ha venido considerando que la seguridad de los usuarios particulares y los consumidores, en todas sus dimensiones, debería ocupar un lugar más central en la reflexión de la Comisión de la UE y la estrategia europea.

En tales términos se han orientado las reformas legislativas, sobre todo las penales, en torno al ámbito económico patrimonial y a la protección de la intimidad y de los datos personales, siendo este último ámbito al que mayor preponderancia se le ha dado por las legislaciones internas de los Estados miembros de la UE y los del Consejo de Europa, y su consideración como objetivos prioritarios, frente al Derecho anglosajón que ha incidido más en el económico patrimonial.

En consecuencia se sostiene que los consumidores y particulares no sólo tienen derecho a estar protegidos de forma realmente eficaz contra los abusos informáticos contra sus datos personales o su privacidad, sino con carácter general a lo que se ha denominado "intimidad informática" o incluso "domicilio informático", que incluye otras modalidades de acciones que deberían ser consideradas ilícitas (aunque no lo son todavía en la muchas de las legislaciones europeas) como el perfilado nominativo abusivo que se realiza mediante programas de espionaje informático (spyware y web bugs) u otros medios, o acciones como la práctica del spamming (envíos masivos de mensajes no deseados) que a menudo se deriva de estos abusos, pues estas intrusiones perjudican a las víctimas tal y como han venido reconociendo la propia UE[1], que llega a considerar que los sistemas de gestión y los programas patentados, cuyo código fuente no está publicado, no ofrecen suficientes garantías de seguridad y protección de la intimidad, sobre todo en el caso de registro de licencias e instalación de patches (parches y actualizaciones) efectuados en Internet, que pueden desviarse para recopilar información sobre los sistemas de cliente-servidor (arquitectura y contenidos, listas de direcciones y conexiones).

Y considerando que tales prácticas van más allá del simple registro del nombre y la dirección del propietario de la licencia del programa para darle una clave de activación o un código de acceso temporal a unos servicios, las mismas constituyen una intrusión y estima deberían prohibirse.

Ante las deficiencias apreciadas en la respuesta legal respecto a la Cibercriminalidad en general, derivada incluso de una

[1] Así los dictámenes del CES sobre la «Propuesta de Directiva del Parlamento Europeo y del Consejo relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión» (DO C 123 de 25.4.2001, p. 50), la «Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior» (DO C 169 de 16.6.1999, p. 36) y la «Incidencia del comercio electrónico en el mercado interior (OMU)" (DO C 123 de 25.4.2001, p. 1).

interpretación jurisprudencial más que excesivamente restrictiva, acomodaticia de los nuevos tipos penales a las figuras tradicionales, surgieron en el ámbito de las comunidades europeas, la Unión Europea y el Consejo de Europa, dos grupos de resoluciones: una tipo Convenio (UE) y otra inclusiva de las decisiones marco (C. de E.).

A) EL CONVENIO CYBERCRIME DE BUDAPEST DE 23.11.2001.

El Convenio de Budapest sobre la Cibercriminalidad del Consejo de Europa, de 23 de noviembre de 2001, y que entró en vigor el 01 de julio de 2004 al haber sido ratificado por 22 Estados, habiéndose ratificado recientemente por España por Instrumento de fecha 20 de mayo de 2010 (B.O.E. de 17.09.10), implica realmente dado su carácter imperativo, un punto de inflexión hacia un tratamiento penal sustantivo, autónomo, unificado y extensivo del fenómeno de la delincuencia o criminalidad informática y telemática, o, utilizando el término acuñado más recientemente, de la cibercriminalidad.

El reiterado Convenio establece una clasificación de los ilícitos informáticos por grupos más novedosa, no siguiendo los patrones clásicos en torno a los bienes jurídicos tradicionales exclusivamente, si bien en algunos aspectos es proclive al confusionismo y al solapamiento de supuestos distintos de ilícitos informáticos bajo una misma figura, debido principalmente a que se trata de una "Convención de mínimos" para poder obtener un amplio consenso entre los diversos Estados que participaron en su confección, algunos incluso ajenos al propio Consejo de Europa como EE.UU, Canadá, la República de Sudáfrica o Japón y a quienes se les había abierto para su intervención y ratificación de la Convención final.

Así recoge en su Título II, sección primera, bajo la rúbrica "Derecho penal sustantivo", las disposiciones, entre otras, relativas a la tipificación armonizada de las conductas que considera penalmente reprensibles en el ámbito de los ilícitos informáticos; nueve infracciones básicas agrupadas en cuatro categorías distintas, una por capítulo:

1.- Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, que comprende las figuras del "acceso ilegal", la "interceptación ilegal", la "interferencia de datos", la "interferencia del sistema", y los "dispositivos ilegales".

2.- Delitos vinculados a la informática, que comprende la "falsificación informática" y el "fraude informático".

3.- Delitos de contenido, que comprende únicamente los "ilícitos relacionados con la pornografía infantil".

4.- "Delitos relacionados con la infracción de los derechos de propiedad intelectual y otros afines".

Es precisamente en el primer grupo, en su art. 2, en el que se prevé la figura del Hacking o Acceso Ilícito como *"acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático"*, significando a continuación que *"cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático"*, que es lo que ha acontecido en la legislación española como veremos.

Pero por el contrario, si bien se hace referencia al delito de pornografía infantil, se omite cualquier referencia al child grooming o acoso infantil, que no fue objeto de análisis ni tratamiento en las Comisiones que redactaron y debatieron el Proyecto de Convenio, al no tener prácticamente incidencia constatable en aquellas fechas (año 2001 y precedentes) sino que la ha tenido con posterioridad.

Así mismo, es significativa la omisión entre las figuras indicadas de mención alguna a una tutela penal específica de los datos de carácter personal, vinculado ello a la presencia de países ajenos al Consejo de Europa, principalmente EE.UU., o a la emisión o difusión en Internet de contenidos ilícitos como el terrorismo, la xenofobia o el racismo, si bien la propia Exposición de Motivos del Convenio justifica tales omisiones en la falta de tiempo para la elaboración de una propuesta asumible por todas las partes, y siendo de considerar que con posterioridad se aprobó un Protocolo Adicional al Convenio (ETS nº 189) relativo a la criminalización de los actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos, y que entró en vigor el 01 de marzo de 2006.

A raíz de lo expuesto y como ya he sostenido con anterioridad en otras ocasiones en los últimos años, en contra de las posturas tradicionales de negación de la realidad del delito informático en su globalidad, y de su conceptuación genérica como meros delitos tradicionales que no representan más que un nuevo modus operandi, esto es el ser cometidos por medios informáticos, o como "delitos contenidos en la vigente legislación cometidos a través de medios informáticos", y superando las nociones conceptuales elaboradas hasta la fecha, como, por ejemplo, la conceptuación de la ciberdelincuencia como equiparable a la financiera, o a una forma de la delincuencia económica, o definiciones parciales del delito informático, el término actual de delito cibernético debe configurarse teniendo como base primaria los nuevos intereses dignos de protección penal como la información y los datos en sí mismos, con uso de conceptos amplios y en torno a lo que ha venido a denominarse delito de datos y/o información.

B) LAS DECISIONES MARCO DEL CONSEJO DE EUROPA DEL 2004 Y 2005.

En cuanto a las resoluciones del Consejo de Europa, que han servido de base a la L.O. 5/2010, de 22 de junio, cabe mencionar en primer lugar la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, en cuyo art. 2 se recogía precisamente que los Estados miembros del Consejo adoptaran las medidas necesarias para la punibilidad como infracciones relacionadas con la explotación sexual de los niños, *de las conductas intencionales siguientes:*

a) coaccionar a un niño para que se prostituya o participe en espectáculos pornográficos, o lucrase con ello o explotar de cualquier otra manera a un niño para tales fines;
b) captar a un niño para que se prostituya o participe en espectáculos pornográficos;
c) practicar con un niño actividades sexuales recurriendo a alguno de los medios siguientes:
i) hacer uso de la coacción, la fuerza o la amenaza,
ii) ofrecer al niño dinero u otras formas de remuneración o de atenciones a cambio de que se preste a practicar actividades sexuales,
iii) abusar de una posición de reconocida confianza, autoridad o influencia sobre el niño.

Y en segundo lugar, y como acto adoptado en aplicación del Título VI del Tratado de la Unión Europea, la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, en cuyo art. 2 se recoge el *Acceso ilegal a los sistemas de información* en los siguientes términos:

1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.
2. Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad.

Con lo que de hecho parecía pretenderse la sanción tanto del *child grooming* o acoso sexual infantil, aunque de forma indirecta al devenir subsumido bajo la figura de la pornografía infantil, como inicialmente el *Hacking*, aunque el apartado 2 delimitaba la concurrencia del requisito de transgresión de medidas de seguridad impuestas que nos aproximaría según cieto sector doctrinal, que considero erróneo, a la figura del *Cracking*.

III.- LA L.O. 5/2010, DE 22 DE JUNIO.

En tales términos, la L.O. 5/2010, de 22 de junio, que entrará en vigor el próximo día 24 de diciembre de 2010, recoge en tres apartados de su Preámbulo, las principales argumentaciones en orden a un tratamiento más pormenorizado de determinadas conductas ilícitas en el ámbito penal informático, en aras a evitar las duplicidades interpretativas que tanto la doctrina como la jurisprudencia venían llevando a cabo de tales comportamientos, y sobre todo al determinar ya expresamente en el Código Penal (CP) unas previsiones tipológicas específicas en orden a aquellos comportamiento que, hasta ahora, quedaban al margen de la antijuricidad penal a tenor de los principios de legalidad, subsidiariedad y mínima intervención penal.

Así el apartado XIII del Preámbulo de la L.O. 5/2010 argumentando en torno a la necesidad de trasposición de la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, crea un nuevo Capítulo II bis en el Título VIII del Libro II del CP dedicado a este tipo específico de delitos y argumenta que "la extensión de la utilización de Internet y de las tecnologías de la información y la comunicación con fines sexuales contra menores ha evidenciado la necesidad de castigar penalmente las conductas que una persona adulta desarrolla a través de tales medios para ganarse la confianza de menores con el fin de concertar encuentros para obtener concesiones de índole sexual", introduciéndose en consecuencia el nuevo art. 183 bis mediante el cual se regula el "internacionalmente denominado "*child grooming*", previéndose además penas agravadas cuando el acercamiento al menor se obtenga mediante coacción, intimidación o engaño".

El apartado XIV del Preámbulo de la L.O. 5/2010, establece como referencia la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, para la resolución de incardinar las conductas punibles en dos apartados diferentes, expresando a continuación "al tratarse de bienes jurídicos diversos":

a) el primero, *"relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno*".
b) El segundo, referente "*al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o*

programas informáticos contenidos en un sistema o en parte del mismo".

Y finalmente el apartado XV se refiere a la separación que en materia de estafas del art. 248 CP, acrecentadas por los fraudes informáticos, del hasta ahora apartado 2, se verifica con la incorporación, separada que no aislada dentro del mismo precepto, de la modalidad defraudatoria mediante utilización de tarjetas ajenas o los datos obrantes en ellas, y que algunos autores incorporábamos dentro del ámbito del fraude informático, o incluso tratábamos últimamente bajo la perspectiva delictual de la "suplantación de la personalidad informática".

Habida cuenta de que tanto la problemática de los ciberdelitos en el ámbito patrimonial y económico va a ser tratada en una posterior ponencia, voy a limitarme en la presente a desarrollar las nuevas previsiones legales de punición del Hawking y del Grooming, como actuaciones propias de la Ciberdelincuencia Intrusiva.

III.- EL HACKING o ACCESO ILEGAL.

Al igual que la figura del hurto o fraude de identidad informática, si bien he venido incluyendo el acceso ilegal o "hacking", entre los ciberdelitos en el ámbito económico-patrimonial, dado que ni la mayoría de la doctrina ni el propio Convenio de Budapest sobre la Cibercriminalidad le otorgan tal naturaleza, sino que suele ubicársele como afectante al derecho a la intimidad personal en el ámbito informático, es por lo que dedico su tratamiento en el ámbito de la cibercriminalidad intrusiva.

El apartado Quincuagésimo tercero del art. Primero de la L.O. 5/2010, de 22 de marzo, recoge en el nuevo apartado 3 del art. 197 CP., el acceso ilegal, en los siguientes términos:

"3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.
Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el art. 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33."

1).- EL ACCESO ILICITO: SIN AUTORIZACION

El término "hacking" tradicionalmente describe la mera entrada o acceso a sistemas informáticos por el mero gusto de superar las medidas técnicas de seguridad, esto es, sin intención o finalidad alguna de manipulación, defraudación, sabotaje, o espionaje. De aquí la necesidad de su tratamiento autónomo, y, además, en una configuración como el ilícito básico de casi todas las restantes modalidades de delitos informáticos, incluyendo los del ámbito económico.

En la práctica esta modalidad de ciberdelito es la más básica y frecuente. Así, por ejemplo, ya se recogía por la doctrina que en una estadística alemana de 1991, los casos de hacking suponían aproximadamente una quinta parte de todos los ilícitos informáticos, siendo su cifra negra o zona oscura muy amplia y extensa, debido a que a menudo las tentativas de lograr el acceso a un sistema informático no pueden ser constatadas ni advertidas.

De hecho, la actividad del mero acceso ilegal o ilícito, también denominado intrusismo informático, no tiene para parte de la doctrina una ubicación específica en un área tradicional de bienes jurídicos protegidos, y si bien se ha venido encauzando el estudio y análisis tal acción ilícita como incidente en el campo de los ilícitos económicos, las respuestas legales en el Derecho comparado lo han venido tratando en otras áreas, principalmente la de los delitos contra la intimidad, como también lo reconoce el propio Convenio sobre la Ciberciminalidad de 2001.

2).- VULNERANDO LAS MEDIDAS DE SEGURIDAD ESTABLECIDAS PARA IMPEDIRLO

La doctrina ha venido posicionándose en torno a la necesidad o innecesariedad de una respuesta penal a tal tipo de comportamientos. Y así, en pro de una no previsión legal penal del hacking, sobre todo en el ámbito económico, se ha venido sosteniendo las reticencias principalmente en torno a la ausencia tanto de un ánimo de lucro económico en el sujeto activo, como de un perjuicio patrimonial efectivo en la víctima o sujeto pasivo de la acción, normalmente titular del equipo, sistema o red objeto de intromisión.

Ciertamente de aceptar la primera observación ni tan siquiera pudiera esta conducta obtener tal calificación como actual delito informático, ni una naturaleza propia. Sin embargo, ya he sostenido con anterioridad que en el hacking sí es de apreciar un ánimo de lucro en el sujeto activo. No es un ánimo de lucro restrictivo o exclusivamente económico, sino genérico o lo que nuestra doctrina y jurisprudencia ha venido considerando y calificando como "animo de lucro jurídico", consistente en la obtención de unas ventajas personales, consistentes

primordialmente en los conocimientos técnicos que la superación de las barreras de seguridad informáticas otorga, de lograr una mayor y más extensa capacidad de libertad de acceso en equipos, sistemas y redes informáticas, de telecomunicación, o telemáticas, sin necesidad de autorización alguna o vulnerando los impedimentos, trabas o mecanismos informáticos de seguridad interpuestos por sus titulares, y finalmente el logro de un "prestigio" o reconocimiento dentro de las cerradas comunidades y colectividades sociales interesadas por las nuevas tecnologías, sus deficiencias y su vulnerabilidad.

Y en cuanto al perjuicio efectivo, debe puntualizarse que si bien en numerosos casos, el titular o usuario informático atacado no resulta efectivamente dañado o perjudicado desde un punto de vista patrimonial o económico en sentido estricto, no obstante sí hay una clara puesta en peligro de los intereses económico-patrimoniales contenidos en los programas o en los datos mismos a los que se tiene acceso, o simplemente en el esfuerzo o coste que le ha supuesto al titular el establecimiento de las medidas de seguridad para evitar tales accesos no autorizados; en estos casos, al menos debe apreciarse que sí se viola o la "formal esfera de la privacidad y del secreto" o "la integridad del sistema informático afectado". O lo que es lo mismo, la vulneración del “domicilio informático” como algunos autores pretenden. Además, en muchos supuestos estas conductas de acceso ilegal aparecen configuradas materialmente como actos preparatorios de comportamientos delictivos informáticos más graves, en donde sí aparecen unos perjuicios considerables, que sucede cuando posteriormente los autores usan su experiencia y los conocimientos adquiridos con sus logros de acceso para cometer o favorecer la comisión por terceros de acciones o actos de espionaje, sabotaje o fraude informáticos.

3).- POR CUALQUIER MEDIO O PROCEDIMIENTO
Actualmente las técnicas de hacking han evolucionado y cada vez más dependen en gran medida de los sistemas de telecomunicación y trasmisión de datos. Las tradicionales formas de hacking en redes informáticas fueron desarrolladas durante los años 80, y se basaban fundamentalmente en la inseguridad en el uso de los "passwords" (contraseñas) de tipo estándar, las cuales a menudo no eran cambiadas regularmente por los usuarios informáticos.

Aunque desde entonces la concienciación sobre la necesaria seguridad tanto de los sistemas y redes informáticos como en el uso adecuado de passwords ha progresado y aumentado, en años recientes Internet ha traído nuevas técnicas de acceso, incluso indirecto o pasivo, en donde es la propia víctima la que actúa "cayendo en las redes operativas latentes" y las activa, tales como IP, DNP, webs simuladas o "web spoofing", o la infiltración en redes informáticas mediante aplicaciones maliciosas en la

web. Estos métodos se han desarrollado con quebranto de los protocolos establecidos para el uso de nuevos sistemas o redes de comunicaciones, como el IP (Internet Protocol) o el HTTP (Protocolo sobre Transferencia de Hipertexto).

4.- A DATOS O PROGRAMAS INFORMATICOS CONTENIDOS EN UN SISTEMA INFORMATICO O EN PARTE DEL MISMO.

Los recientes desarrollos de la tecnología telefónica y de telecomunicaciones han conducido al hecho de que hoy en día el hacking no solamente afecte a sistemas informáticos clásicos sino cada vez más también a líneas telefónicas, contestadores telefónicos, sistemas de correo de voz e incluso aparatos de telefonía móvil. Ya tradicional y casi anticuado es el uso las denominadas "cajas azules" ("blue box") y otros aparatos de señales, que los "hackers telefónicos" conectaban en las centrales telefónicas locales de la compañía de teléfono y están en disposición de escuchar digitalmente las conversaciones de la zona "pinchada" de una localidad.

Incluso otras informaciones confidenciales o codificadas, especialmente de los números de tarjetas de acceso telefónico (denominadas tarjetas prepago) son obtenidas por estos métodos y posteriormente revendidas. La red digital ISDN y la combinación de teléfono y tecnología informática, con telefonía móvil que incorpora sistemas informáticos con acceso a Internet, ya suponen nuevas formas de comisión, no sólo abusivas sino plenamente ilícitas y delictivas.

Un ejemplo clásico de esta forma de hacking telefónico es un caso de 1992 aludido por **SIEBER**, en el que unos jóvenes alemanes penetraron en el ordenador de voz del Barclays Bank en Hamburgo a la cual los clientes del banco informaban del recibo de sus tarjetas de crédito incluyendo el correspondiente número de identificación personal así como anuncios en caso de pérdida o -dando el respectivo número secreto- cuando pedían un aumento de sus límites de crédito, logrando con tal intervención la información referente a tales datos confidenciales para su posterior uso ilícito[2].

En tales términos y frente al posicionamiento de ciertos sectores doctrinales respecto a la no incriminación penal autónoma del hacking, considero que la misma es precisa tanto de conformidad con las vigentes recomendaciones internacionales, como atendida la gravedad del riesgo y peligro que supone tal conducta o acción no sólo para el ámbito patrimonial y de la intimidad de la víctima, sino también para el preciso grado de fiabilidad y confianza de la sociedad, de la colectividad

[2] Cita recogida por dicho autor del diario "Der Spiegel" nº. 34/1992, págs. 206 y ss.

social, en la seguridad, seriedad, y veracidad de los datos, la información y los medios y redes por donde se comunican, transfieren o captan, y que han venido corroborando los sucesos y casos más recientemente descubiertos y de los que se han hecho eco los medios de comunicación, y de cuyo alcance va tomando ya conciencia la sociedad en la actualidad[3].

Ahora bien, esta modalidad delictiva, desde la perspectiva de su configuración como delito base o básico de los delitos de riesgo informático y de la información que he venido defendiendo desde hace años, realmente no coincide con el concepto tradicional dado de *"acción de acceder, sin autorización y de forma subrepticia, a un sistema o red informática o telemática, así como la interferencia no autorizada de un proceso de transferencia o comunicación electrónica de datos"*.

En España hasta la L.O. 5/2010, de 22 de marzo, no ha habido una reacción normativa penal específica contra el hacking, a pesar de que algunos autores, como **GUTIERREZ FRANCÉS** o **MORON LERMA** han pretendido encajar esta modalidad delictiva, aunque reconozcan que de forma problemática y forzada, en la figura delictiva del art. 256 CP, u otros como **DE ALFONSO LASO**, lo pretendan respecto de algunos supuestos de lo que denominan "hacking blanco", en la figura preexistente del artículo 197 CP. Pero es que tales primeras autoras contemplan al denominado intrusismo informático no sólo como el "conjunto de comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicación electrónica de datos", sino también "*la utilización de los mismos sin autorización o más allá de lo autorizado*", y por tanto ampliando el concepto de hacking a otros supuestos como el de hurto de tiempo compartido, el de servicios o el de uso no autorizado de ordenador, casos que son más propios de ubicar en la modalidad de hurto de tiempo informático, y frente al cual sí puede estimarse como aplicable la figura delictiva defraudatoria del art. 256 citado.

Además hasta la L.O. 5/2010, de 22 de junio, conforme al artículo 270, párrafo tercero, CP podía pretenderse la sanción como delito de determinados actos preparatorios de lo que pudieran ser algunas modalidades de hacking, como en similares términos se sanciona la tenencia de útiles para falsificar, al construirse como conducta delictiva "la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador". Y ello es así por cuanto si bien, como sostiene **QUINTERO OLIVARES**, la

[3] Ver artículo ¿Ciberactivistas o ciberdelincuentes?, El país, suplemneto vida & artes, miércoles 20 de octubre de 2010, pags 30 y 31.

inclusión de esta figura en el Código Penal es consecuencia de la Directiva 91/250/CEE, de 14 de mayo (DOL núm. 122, de 17 de mayo de 1991 [LCEur 1991, 475]), del Consejo de las Comunidades Europeas, sobre protección de programas de ordenador desarrollada en los arts. 95 a 104 de la Ley de Propiedad Intelectual, al no exigirse ningún elemento subjetivo específico del injusto, concretamente la finalidad de atentar contra la propiedad intelectual, que indebidamente se presume por algún autor dada la ubicación sistemática del precepto, considero que no existe óbice alguno a tenor de su redacción para ser aplicado a aquellos supuestos en los que el medio o instrumento, que puede ser incluso un programa informático en sí mismo, está destinado a anular, suprimir o quebrantar los dispositivos de software informático de seguridad instalados en sistemas o redes informáticas o la interceptación de procesos de transferencia electrónica de datos, y lograr el acceso a los mismos.

Es de reseñar un caso clásico que sería subsumible, si se hubiera producido en nuestro país, en la conducta tipificada en este art. 270, párrafo tercero. Me refiero al caso[4] que dio lugar a la detención por la policía noruega a finales del mes de enero del 2000 de un joven noruego de 16 años (J.L.J.) que, a través de la página web de Internet www.mmadb.no, dominio del que era titular su padre, también acusado por las autoridades, ofrecía gratuitamente un programa (DeCSS, desencriptador para Linux) que permitía descifrar la información contenida en un D.V.D. (Disco Versátil Digital) pudiendo consecuentemente ver en el ordenador las películas contenidas en un D.V.D. sin necesidad de comprar un lector. Si bien la tecnología del D.V.D. ya apareció para el público en general en 1995, y en 1997 ya aparecieron los primeros casos de copias de películas contenidas en tales soportes, hasta septiembre de 1999 no se había logrado acceder a la información en sí misma, encriptada con el algoritmo CSS. En tales fechas al menos dos grupos europeos de piratas informáticos (Masters of Reverse Engineering, "MoRE", y Drink or Die, "DoD") lograron quebrar la protección de la información, el sistema de encriptación, precediéndose a su ofrecimiento gratuito a través de Internet.

Dado que el citado programa DeCSS al publicar el código tiene también como otras características el permitir fabricar reproductores y nuevos programas para D.V.D. sin pagar licencias o el que D.V.D. para el mercado americano puedan verse en Europa, al poderse cambiar el número de zona y saltarse así las restricciones de las casas productoras, la reacción de la industria no se hizo esperar y en diciembre del mismo año se interpusieron tres pleitos ante los Tribunales norteamericanos contra docenas de personas que ofrecían el reiterado programa o

[4] Publicado entre otros en "El País", jueves 03.02.00, ciberp@ais, pág. 12.

enlaces en Internet. La Justicia norteamericana dio la razón en Enero del 2000 a dichas corporaciones al considerar que el sistema D.V.D.-C.S.S. tenía la calificación jurídica de secreto industrial. Pues bien, la mera acción de tenencia de tal programa, no siendo el autor quien hubiera vulnerado el sistema de protección encriptada del sistema D.V.D., pudiera encuadrarse en el reiterado párrafo tercero del art. 270, aunque fuera para la visión de una película en D.V.D. que se hubiera adquirido legalmente. ¿Pero y su uso? ¿No podemos considerar una incongruencia normativa y un quebranto del principio de mínima intervención penal la tipificación de esta conducta pero la impunidad del uso de tales medios al no estar sancionada, hasta la entrada en vigor de la LO 5/2010, la conducta del intrusismo informático?

Es por tanto que resultaba como mínimo ilógico desde el punto de vista sistemático que se castiguara esta conducta y no así expresamente la fase siguiente, ya ejecutiva de hacking, de uso o utilización de dichos medios para acceder a un equipo, sistema o red informática o de telecomunicación, cuando no van dirigidos específicamente a atentar contra la propiedad intelectual, y se prevean como figuras delictuales fases posteriores o postejecutivas del propio acceso ilegal, cuando se efectúan manipulaciones, alteraciones, copia o sustracciones de la información o de los datos a los que se tuvo acceso de forma ilícita.

Podemos afirmar en resumen que si se ha hecho precisa la tipificación de este comportamiento, pues es preciso reconocer y superar la ausencia de una respuesta eficaz a través de otros cauces, como la autoprotección, seguridad y medidas legales civiles o administrativas, constatada por lo demás a tenor de la experiencia criminológica expuesta, y el que pretendamos por vía interpretativa pretender sancionar tales acciones en las figuras delictuales creadas ex novo por la posibilidad de subsumir en la acción típica preexistente bien un acto preparatorio del hacking, bien el inicio de la fase ejecutiva delictual, es decir como tentativa, de un ilícito más grave (espionaje, sabotaje o defraudación informática) cuando pudiera constatarse la existencia del elemento específico del injusto concreto requerido en cada caso.

Pero hay que evitar los dos extremos: intervención mínima, sí, pero suficiente. Y ello sucede en este tipo de acciones, deviniendo en necesaria la introducción de la figura específica del intrusismo informático, acceso ilegal o hacking, de carácter general y global. Y ello no supone realmente ni una sobrecriminalización, ni una "huida hacia el derecho penal", sino la respuesta adecuada para hacer frente a los graves riesgos y peligros que tales acciones suponen para bienes individuales y colectivos, sin necesidad de una posterior

vulneración de la propiedad intelectual, industrial, o la existencia de un perjuicio económico o patrimonial efectivo, o un ánimo específico de atentar contra tales bienes jurídicos tradicionales.

IV.- EL GROOMING o "CHILD GROOMING", o ACOSO SEXUAL A MENORES.

El ya referido apartado XIII del Preámbulo de la L.O. 5/2010 al referirse al bien jurídico protegido por los delitos sexuales cometidos sobre menores, alude a "una dimensión especial –del mismo- por el mayor contenido de injusto que presentan estas conductas", y si bien conceptúa la indemnidad sexual como "el derecho a no verse involucrado en un contexto sexual sin consentimiento válidamente expresado", incluye dentro de dichos bienes jurídicos protegidos "la formación y desarrollo de la personalidad y sexualidad del menor", creándose un nuevo Capítulo II bis en el Título VIII del Libro II del CP denominado "De los abusos y agresiones sexuales a menores de trece años", y en el que junto a una nueva redacción del art. 183, se introduce el nuevo art. 183 bis regulador del "Child Grooming" (acoso infantil).

Por acoso infantil hay que entender todo conjunto de "acciones deliberadas cometidas por un adulto, con el fin de ganarse la confianza de un menor, crear una conexión emocional, y con ello lograr disminuir las inhibiciones o reticencias del menor, para iniciar una relación sexual, primero virtual y posiblemente después física".

El child grooming a través de las TIC se ha extendido significativamente por cuanto los conceptos de seguridad y privacidad en los jóvenes, han evolucionado. Así hay menos reticencias a compartir datos personales (70% perfil público, cuantos más amigos, mejor); ha cambiado el concepto de "conocido", deviniendo en otro totalmente aleatorio; y se explica asimismo en la forma en cómo se acercan los menores a Internet (como una extensión de la vida real) y con reserva activa de sus acciones y contactos con sus padres y tutores, y en muchos casos incluso reserva pasiva de éstos a conocer los contactos, relaciones y movimientos de sus hijos en la Red.

Y ello se refleja en un estudio reciente de este año 2010 de la red *EU Kids Online* que aseveraba tres notas fundamentales:

a)- Que el 29% de los niños europeos de entre 9 y 16 que usan Internet, se ha comunicado en el pasado con alguien que no conocía cara a cara previamente.

b)- Que el 61% de los padres de niños/as que han conocido en la vida real personas contactadas online dicen que su hijo/a no lo ha hecho.

c)- Que en España un 8%de los menores españoles en alguna ocasión han quedado cara a cara con alguien a quien sólo conocían previo contacto en Internet; siendo que un 20% de los menores aseguran contactar online con gente que no conocen en la vida real.

Esquemáticamente podemos diferenciar las siguientes fases sucesivas en el grooming:

a) Fase de amistad.
b) Toma de contacto, gustos, preferencias. Confianza.
c) Fase de relación.
d) Confesiones personales e íntimas. Consolidación.
e) Componente sexual.
f) Participación actos naturaleza sexual, fotografías, webcam.
g) Extorsión
h) Escalada de peticiones.
i) ¿Agresión?

En cuanto a su marco legal punitivo, si bien hasta ahora podía venir siendo punible aunque no de forma individualizada y diferenciada, ni aún menos en cuanto a su verificación a través de TIC, y con posturas o posicionamientos doctrinales e incluso respuestas jurisprudenciales antagónicas, subsumiéndose en otras figuras delictivas como el exhibicionismo, la corrupción de menores, las amenazas, el abuso sexual, la agresión sexual, etc., pero obviando la estricta protección del menor en el acoso al que era sometido, así como la sucesión de los hechos que configuran el ilícito a configurar, ello cambia sustancialmente con la introducción del art. 183bis en el CP.

Dicho precepto sanciona al "*que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de 13 años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189* (esto es delitos contra la libertad e indemnidad sexual, con exclusión de los de exhibicionismo y provocación sexual, así como los delitos relativos a la prostitución de mayores de edad)*, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de 1 a 3 años de prisión o multa de 12 a 24 meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño*".

De un análisis de los elementos objetivos y subjetivos del tipo del injusto se desprende que:

a) es una conducta dolosa, no cabiendo su comisión imprudente.

b) el sujeto activo puede ser cualquiera mayor de edad (18 años).

c) los medios a utilizar son tanto Internet, como el teléfono, como cualquier TIC.

d) la acción a desarrollar consiste en:
1.- contactar con un menor de 13 años (con lo que deberá acreditarse que el sujeto activo tiene conocimiento de la edad del menor, por cuanto lo contrario devendría en la atipicidad de la conducta por una ausencia o error de dolo sobre los elementos del tipo y la imposibilidad de sanción penal de la conducta, ni tan siquiera conforme al art. 14 CP., al no existir modalidad imprudente de este delito)
2.- proponerle el concertar un encuentro con el mismo.
3.- verificar el concierto con el fin (elemento específico subjetivo del tipo del injusto) de cometer un delito contra la libertad o indemnidad sexual de los arts. 178 a 183 y 189. Hay que recordar que se trata de supuestos de agresiones y abusos sexuales y utilización de menores o incapaces en espectáculos exhibicionistas o pornográficos y en la elaboración de material pornográfico. Se entiende que es la libertad e indemnidad sexual del menor, pero, en los términos en que viene prescrito el precepto, cabe plantearse si pudiera ser factible para cometer el delito sexual contra un tercero? La respuesta debe ser negativa por cuanto el legislador lo que busca con el precepto es la protección de los menores frente a las personas adultas que a través de los medios indicados buscan la confianza de éstos concertando encuentros con la finalidad de conseguir actividades sexuales, y en este caso devendría la adecuada subsunción punitiva en el delito sexual cometido o pretendido cometer contra dicha tercera persona. Aunque para la consumación del ilícito no es preciso el que llegue a verificarse este nuevo delito, perteneciendo su comisión a la fase de agotamiento delictual.

e) que la acción de proponer expuesta en la letra precedente venga acompañada, esto es, seguida, de otro acto material encaminado al acercamiento. Y ello hay que entenderlo como el desplazamiento de ambas partes o de una de ellas, para contactar personalmente en algún lugar, siendo preciso para la consumación del delito el que el adulto llegue a un acuerdo con el menor para reunirse con él.

f) las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.

V.- CONCLUSIONES.

1ª.- El ciberdelito se presenta no sólo como manifestación global y genérica de la criminalidad informática originada por el riesgo propio del uso y utilización de la informática, la telemática y de la información en la actual sociedad, y por tanto como categoría funcional o criminológica, sino además como concepto para referirnos a un conjunto de figuras substantivas normativas de tipos delictivos con entidad y sustantividad propia, y que conformarían el núcleo de lo que he venido formulando como Derecho Penal Global del Riesgo Informático y de la Información, en donde el delito informático strictu sensu viene configurado como un delito pluriofensivo, en el que hay que tener siempre concurrente la protección de los nuevos intereses derivados de la sociedad global del riesgo informático y de la información (la información en sí misma, los datos informáticos, que son la representación de aquélla, y la fiabilidad y seguridad colectiva en los medios y sistemas de tratamiento y transferencia de la información).

2.- La L.O. 5/2010, de 22 de junio, incorpora las nuevas tipificaciones del Hawking y del Grooming no en orden al Convenio sobre la Ciberdelincuencia de 23.11.01 de la U.E. suscrito por España, y ratificado mediante Instrumento de 20 de mayo de 2010, aunque publicado en el BOE del 17.11.10 (con casi 10 años de retraso o tardanza) sino en base a las directrices instauradas en dos Decisiones Marco del Consejo de Europa más recientes: la Decisión Marco 2004/68/JAI, de 22 de diciembre, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil; y la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

3ª.- Resultaba precisa la tipificación del Hacking tanto de conformidad con las vigentes recomendaciones internacionales, como atendida la gravedad del riesgo y peligro que supone tal conducta o acción no sólo para el ámbito patrimonial y de la intimidad de la víctima, sino también para el preciso grado de fiabilidad y confianza de la sociedad, de la colectividad social, en la seguridad, seriedad, y veracidad de los datos, la información y los medios y redes por donde se comunican, transfieren o captan.

4ª.- El tipo del art. 183 bis CP no se ajusta a las previsiones fácticas usuales de lo que venía considerándose acoso sexual de menores o Child Grooming y requiere demasiados elementos objetivos sucesivos, cuando no simultáneos para su consumación, que su apreciación judicial, como delito de mera actividad con ese elemento subjetivo finalista del injusto (a fin de cometer cualquiera de los delitos descritos en lo arts. 178 a 183 y

189), va a devenir en su limitada aplicación, y en la mayoría de los casos apreciable sólo como forma imperfecta de ejecución, cuando no objeto de apreciaciones contradictorias de la jurisprudencia menor dados los términos ambiguos que contiene en su redacción tipológica y que requerirán de una interpretación restrictiva jurisprudencial penal en base a los principios de mínima intervención, subsidiariedad e incluso última ratio, a fin de no vulnerarse el principio de seguridad jurídica.

Barcelona, noviembre de 2010.

Enrique Rovira del Canto
Magistrado
Doctor en Derecho
Licenciado en Criminología
Profesor de Derecho penal