EGUZKILORE
Número 20.
San Sebastián
Diciembre 2006
151 - 161

LA PERSECUCIÓN Y SANCIÓN DE LOS DELITOS INFORMÁTICOS

Carmen ADÁN DEL RÍO
Fiscal del Tribunal Superior de Justicia del País Vasco

Resumen: Cada vez con más fuerza se incorpora a nuestra vida cotidiana el uso de las nuevas tecnologías, convirtiéndose en algo habitual, no exclusivo de determinados profesiones. Esto conlleva la utilización de este nuevo medio para cometer delitos, transformándose en un fenómeno creciente de riesgo y perjuicio, quedando muchos tipos penales como insuficientes. Desde esta perspectiva se reflexiona sobre la falta de un concepto único de delitos informáticos, los problemas de interpretación de los tipos penales, la necesidad o no de un tratamiento autónomo de estos delitos, así como las dificultades de su investigación y prueba.

Laburpena: Geure eguneroko bizitzan indartsu sartu dira teknologia berriak, ohikoak bihurtuz eta ez bakarrik zenbait lanbidetan. Bide hau erabiltzen dute askok delituak egiteko, era honetan arrisku eta galera fenomenoa sortuz, eta honela zenbait tipo penal gutxiegizko bihurtuz. Ikuspegi honetatik, delitu informatikoen gaineko kontzeptu bakarraren falta somatzen da, delitu hauen trataera autonomoaren beharra edo ez, eta bere ikerkuntza eta frogaren zailtasunak.

Résumé: l'utilisation des nouvelles technologies s'incorpore à notre vie quotidienne de plus en plus, pour devenir habituelle et non exclusive de quelques professions. Ceci entraîne l'utilisation de ce nouveau moyen pour commettre des infractions, en devenant un phénomène de risque et préjudice, et les types pénaux semble être insuffisants. Du ce point de vue on réfléchit sur l'absence d'un concept unitaire de délit informatique, sur les problèmes d'interprétation des types pénaux, sur la nécessité ou non d'un traitement autonome pour ces infractions, ainsi que sur les difficultés de son enquête et preuve.

Summary: New Technologies are increasingly present in everyday life, and have become something usual, not exclusive to some professionals. This implies the use of these resources to commit crimes, what has become an increasing phenomenon of risk and damage, and reveals that some penal types could be inadequate. From this point of view, some reflections about the lack of an unanimous concept of computer crimes, the problems interpreting penal types, the need (or no need) of an autonomous treatment for these crimes, and the difficulties in investigating and getting evidence are presented.

Palabras clave: Criminología, cibercriminalidad, nuevas tecnologías, delitos informáticos, Derecho penal.

Hitzik garrantzizkoenak: Kriminologia, ziberkriminalitatea, teknologia berriak, delitu informatikoak, zuzenbide penala.

Mots clef: Criminologie, cybercriminalité, nouvelles technologies, délits informatiques, Droit pénal.

Key words: Criminology, Cyber-crimes, new technologies, computer crimes, criminal law.

INTRODUCCIÓN

La experiencia nos demuestra, que hoy en día, pocos ciudadanos viven al margen o sin contacto directo o indirecto con un medio informático. Y cada vez, con mas fuerza la utilización de Internet se ha convertido en algo habitual, no exclusivo de determinadas profesiones.

De hecho, no resulta exagerado afirmar que de cara al futuro generamos una dependencia creciente a estos medios, siendo su incorporación a nuestra vida cotidiana, algo tan evidente, que pronto ésta se verá notablemente dificultada sin su apoyo. Desde el momento en que las empresas lo incorporan casi inevitablemente a su funcionamiento, o que nosotros lo introducimos en los aspectos más insospechados de nuestra vida, queremos como ciudadanos, la cobertura de nuestros derechos en ese ámbito.

Cuando se alerta al ciudadano de que su patrimonio, su intimidad u otros derechos pueden verse afectados por el uso de las nuevas tecnologías, pocos se preguntan cuál es la fórmula adecuada con la que el legislador debe protegerles. Cabe pensar que el Código Penal, con el catálogo de bienes jurídicos en él recogidos, resulta suficiente para dar respuesta a esta demanda de seguridad en el uso del ordenador o en la navegación en red. Sin embargo, la realidad alerta de un fenómeno creciente de riesgo y perjuicio, que debiera llevarnos a no dejar el debate como zanjado, cuando muchos de los tipos penales resultan insatisfactorios y excluyen conductas que no debieran quedar fuera.

Desde esta perspectiva, pueden ser objeto de reflexión varios temas:

I.- La falta de un concepto único de delitos informáticos.

II.- Los problemas de interpretación que presentan los tipos penales existentes.

III.- La necesidad o no, de un tratamiento autónomo de los delitos informáticos.

IV.- Las dificultades de investigación y prueba de estos delitos.

I. FALTA DE UN CONCEPTO ÚNICO DE DELITOS INFORMÁTICOS

Los Fiscales en nuestra Memoria anual, al igual que los jueces, carecemos de una adecuada estadística de los delitos informáticos. El hecho de que no exista un título en el Código Penal sobre delitos informáticos o contra un bien jurídico concreto relacionado con la informática, dificulta extraordinariamente aportar datos concretos en la materia. Es más, no sólo tenemos dificultades para cuantificar exactamente el número de estos delitos, sino que incluso discutimos a veces sobre que incluir en ese término. Por ello, aunque en la Memoria anual se suelen seguir los títulos, capítulos y secciones del Código Penal, cuando se hace preciso algún estudio o estadística concreta, utilizamos un concepto mixto en el que incluimos,

– por un lado, las acciones que atacan los sistemas informáticos,

– y por otro, las acciones realizadas a través del ordenador. Dentro de este segundo grupo se da una especial importancia a las que atentan contra bienes jurídicos de mayor calado, como las relativas a la pornografía infantil, aunque sin dejar de lado, como es lógico, las restantes, ya sean de carácter patrimonial, amenazas, blanqueos…

Esa falta de concepto único nos impide utilizar adecuadamente las herramientas estadísticas que, para cualquier seguimiento o decisión de futuro, son cada vez más necesarias. Así como la estadística nos demuestra el avance o retroceso cada año de los robos en domicilio, o de los robos con llaves falsas, cuando intentamos conocer cuántos delitos de los que atentan contra un bien jurídico concreto son realizados por medios informáticos o utilizando Internet, nos encontramos una barrera de método estadístico de difícil solución. Barrera que tiene su origen en que el registro informático de los delitos se realiza como indicábamos anteriormente siguiendo la estructura y sistemática del Código Penal.

En conclusión, en tanto no se modifiquen el sistema de registro informático de Fiscalías y Juzgados, atendiendo o demandando este criterio, resulta prácticamente imposible afirmar de forma exacta o cuando menos suficientemente fiable, la evolución de la delincuencia informática (a salvo quizá de algunos artículos concretos, como, entre otros, el 197 CP).

De todos modos, sí es posible constatar grosso modo, por la propia muestra que nos da el trabajo diario, que se ha producido un aumento significativo de lo que denominamos delincuencia informática patrimonial, esto es, la que utiliza los sistemas o procedimientos informáticos para obtener una ganancia o un quebranto evaluable económicamente. Curiosamente, y siendo mucho más graves otros ataques, como la pornografía infantil, lo cierto es que su descubrimiento y su inclusión en procedimientos penales es aún escasa y difícil. Incluso se podría añadir, como indicaba anteriormente, que no hay un número relevante de denuncias o investigaciones por intromisiones o ataques a sistemas informáticos, a salvo de aquellas que han causado un perjuicio patrimonial en cuantías más o menos relevantes.

II. LOS PROBLEMAS DE INTERPRETACIÓN QUE PRESENTAN LOS TIPOS PENALES EXISTENTES

El tratamiento actual, en lo que se refiere a los tipos penales más significativos y novedosos, entronca con el tratamiento constitucional de la informática. Así, el artículo 18.4 de nuestra Constitución, aborda la informática, desde la perspectiva de la intimidad personal y familiar, señalando "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".* Con ello, la informática, se plantea en palabras de Garrido Falla, como una nueva técnica que, siendo útil, ocasiona numerosos problemas a la hora de garantizar los derechos individuales, sobre todo y en su origen, por razón de los efectos que sobre la vida privada puede tener la concentración de datos que esta técnica o medio permite. En resumen, y fundamentalmente se incide en la protección de la privacidad, y el derecho al acceso a los datos (art. 105 CE).

Ahora bien, este mismo autor señalaba que, aunque el acento se coloque en garantizar la intimidad, se está reconociendo la dificultad de delimitar todos los bienes jurídicos afectados, por lo que el texto constitucional en realidad ha extendido la protección a todos los derechos, siendo altamente significativo el comentario de Pérez Luño al mencionado artículo 18, cuando reconoce, que *"en razón de su propia ambigüedad, se da pie a una interpretación amplia, progresiva, o si se quiere alternativa del precepto".*

La mayor parte de los delitos del CP de 1995, que tratan el tema, lo hacen, pues, como *modalidades de acción* por medios informáticos (y publicidad engañosa, pornografía infantil...). Sucede, sin embargo, que cuando se aborda el supuesto de hecho al objeto de encuadrarlo en el tipo penal, la tendencia a intentar comprender la acción o el medio, desde premisas e interpretaciones pensadas para otras modalidades o medios no informáticos, se convierte en obstáculo para realizar correctamente la integración. Las dificultades se presentan incluso con los nuevos tipos penales, como por ejemplo, el art. 197 del CP, que recoge conductas típicas que afectan al secreto, a la intimidad, a la imagen, y a los datos reservados o de carácter personal o incluso las comunicaciones. Artículo, dentro de lo que cabe, que, al no exigir producción real de perjuicio en el apoderamiento de los datos contenidos en ficheros o soportes informáticos, facilita la acreditación de la acción y la autoría, aun cuando haya de incidirse en el elemento subjetivo de saber y querer actuar en perjuicio del titular de los datos o de un tercero. Pero que, precisamente por el título donde se encuentra, protege frente a la exposición o ataque sólo contra los datos que un hombre medio de nuestro entorno y cultura considera sensible, por ser inherente al ámbito de su intimidad, y no frente a otras intromisiones.

La jurisprudencia oscila, mezcla conceptos de privacidad e intimidad, no reconociendo como delito determinados accesos ilícitos, que provocan una sensación de perplejidad en el ciudadano que forzosamente tiene que desmotivar a la hora de que empresas y particulares acudan a los Tribunales. Un ejemplo, lo es la STS 1916/2006 que, en supuesto que afectaba a la Administración Pública, y después de múltiples incidencias, llegó a la absolución, considerando, *que la actuación enjuiciada no puede considerarse ética ni jurídicamente indiferente, y que las comunicaciones fueron interferidas de forma ilegítima, pero no pueden calificarse como delito, puesto que, así como los particulares y las empresas privadas pueden ser titulares del derecho a la intimidad, este bien jurídico es esencialmente incompatible con las normas que regulan la actividad de la Administración Pública, que se rige irrenunciablemente por los principios de publicidad y transparencia, por lo que la Administración no puede ser sujeto pasivo del tipo penal descrito en el artículo 197.1 del Código penal"*.

La pregunta que nos hacemos es si, hoy en día, sigue siendo admisible que las actuaciones abusivas u otras intromisiones, o cuando los datos no pueden ser considerados totalmente reservados o pertenecientes a la esfera de la intimidad, queden fuera del Código Penal, por mucho que éste sea ultima ratio.

En esta línea de argumentación, entre los ejemplos de la insuficiencia de los tipos penales actuales, está la contradictoria jurisprudencia sobre los hackers. Con relación a los hackers, piratas informáticos buenos que entraban en accesos restringidos por razones de mera diversión, constan numerosos pronunciamientos absolutorios, frente a los llamados crackers, que entraba con fines criminales o vandálicos. Como excepción, sí consta algún pronunciamiento condenatorio en Juzgado de lo Penal, como el caso de quien entró en la red de administración de un juego informático de pago vía Internet, utilizando para ello una cuenta interna permitida por el administrador de programa para los empleados de la empresa, que suponía obtener los códigos binarios y la disposición absoluta sobre al acceso al juego, con lo que además podía cambiar incluso las reglas y disfrutar libremente del juego.

La resolución reconocía la existencia de varias sentencias que señalaban que en nuestro sistema penal no aparece tipificada de manera expresa y autónoma la figura del hacker, pero, según su razonamiento, ello no implica que no se le pueda encuadrar en alguno de los tipos penales, entre ellos, el artículo 197 del CP. Esto es, si al navegar por la red se averiguan las claves de acceso a un sitio y se quebrantan, entrando al lugar, en realidad se están descubriendo los secretos de otros, la esfera de privacidad. Es más, el dolo de descubrimiento de los secretos, entienden estas sentencias, se puede dar por probado por el quebrantamiento de las claves de acceso a las contraseñas, porque esa contraseña está marcando una esfera de privacidad y al final el dolo en estas conductas se ha de reconducir al conocimiento y voluntad de invadir la esfera de privacidad que representa la colocación de una contraseña de acceso. Finalmente se daba por probado el 197,1, pero no el número dos en el que se constata el perjuicio; resolución que apunta quizá a lo que se demanda por la sociedad, pero que contradice el criterio jurisprudencial sobre el bien jurídico al que responde dicho artículo.

Las oscilaciones han llegado hasta el punto que, recientemente, los medios de comunicación presentaban como una de las grandes novedades del proyecto de reforma del Código Penal, que, por fin, se penalizará la actuación de los piratas informáticos, puesto que *"es necesario actualizar y modernizar la respuesta penal ante determinados delitos que se producen en sectores nuevos, producto de los últimos avances tecnológicos..."*, caracterizando como delito las intromisiones ilegales en sistemas informáticos ajenos, admitiendo, pues, que el supuesto de hecho no estaba suficientemente definido, dando lugar a muy diferentes y contradictorias resoluciones judiciales.

Tampoco se puede decir que el problema se da sólo con relación a tipos penales novedosos como el 197 CP, sino que, para mayor sorpresa, tipos penales relacionados con los medios informáticos, relativamente pacíficos en su interpretación, se encuentran nuevamente cuestionados. El ejemplo más significativo se refiere a algo aparentemente superado, como era la discusión sobre el uso en cajeros automáticos de tarjetas sustraídas a sus propietarios. Discusión que se centraba en calificar el hecho como estafa informática o como robo.

Ya en la Memoria de 1987, cuando se hacía mención a la proliferación de este tipo de conductas y se daban instrucciones de cómo enfocar su persecución, se calificaba el supuesto como robo con fuerza entendiendo que había utilización de llaves falsas. Esa calificación inicial partía de considerar que no se daban los elementos de la estafa, puesto que no se puede engañar a una máquina, y el cajero automático no puede ser inducido a error puesto que funciona como estaba programado, entregando el dinero a quien introduce la tarjeta y marca el número clave. Posteriormente, a pesar de que se introdujo específicamente junto al tipo básico de la estafa, en el nº 2, la estafa informática, se siguieron dictando sentencias en las que este supuesto se recogía como robo. Recientemente el TS ha dictado una sentencia, la nº 185/2006 de 24 de febrero, quizá algo extraña porque termina absolviendo, pero en la que se dice: *Cabe pensar hipotéticamente, que el uso abusivo de tarjetas que permiten operar en un cajero automático puede ser actualmente subsumido en el 248.2 (la estafa informática), dado que tal uso abusivo constituye un artificio semejante a una manipulación informática, pues permite lograr un funcionamiento del aparato informático contrario al fin de sus programadores.*

Ante nuevos recursos pendientes, la situación es otra vez de estar a la espera para determinar si es un cambio de posición jurisprudencial o un obiter dicta sin mayor transcendencia; pero en todo caso, ello refrenda la idea de que no pisamos suelo firme, cada vez que el medio informático se incluye en un tipo penal.

Es cierto que, la utilización de los tipos penales tradicionales para supuestos de hecho relacionados con la informática tiene sentido en ocasiones, o se cubre con referencias como la del artículo 26 CP sobre el documento informático (*todo soporte material que exprese o incorpore datos o hechos con eficacia probatoria o relevancia jurídica, da plena vigencia penal al documento informático),* lo que nos permite aplicar toda la doctrina sobre las falsedades a los casos de falseamiento de documentos y registros informáticos. De hecho, en nuestro trabajo diario, vemos alegaciones o pronunciamientos que intentan convertir los artículos dedicados a las falsedades en un tipo al que recurrir, cuando muchos de esos casos no puedan reconducirse a los tipos específicamente informáticos. Una especie de cajón de sastre que impida la impunidad.

La sensación final que nos queda en la práctica diaria es que la realidad, como siempre es más rica en supuestos de lo que el legislador va previendo, mostrándonos acciones nuevas que no encajan en los tipos penales, sino con un exceso de voluntarismo, que no está claro sea recomendable en el ámbito penal.

III. NECESIDAD O NO DE UN TRATAMIENTO AUTÓNOMO DE LOS DELITOS INFORMÁTICOS

Es conocida, y quizá todavía aceptable, la posición de quienes sostienen que, en la mayor parte de los casos, la informática e Internet ha provocado diferentes modalidades delictivas por razón de los medios empleados o del lugar donde se desenvuelven, siendo estas modalidades un ataque más que se produce a los bienes jurídicos tradicionales. En este sentido, la no existencia de un título específico en nuestro Código Penal que acoja este tipo de delitos se considera un acierto del legislador de 1995.

Igualmente ha tenido un importante peso el argumento de que existen medios fuera de la ley penal para responder frente a los ataques más llamativos, y que la posible consideración como infracción y consiguiente sanción de carácter administrativo sería cobertura suficiente para la demanda actual de protección en este ámbito de actuación del ciudadano.

Pero, no siendo partidaria en la mayor parte de los casos de lo que se viene denominando desbordamiento del ámbito penal o adelanto de la barrera de protección penal (según la posición que ocupa quien lo alega), ni de la extensión desmedida de los tipos penales, tengo la sensación, de que el problema crece y no se soluciona. El aumento desmedido de vehículos y sus riesgos provocaron, en su momento, el reconocimiento en el Código Penal de la seguridad vial como bien jurídico digno de protección, entendiendo el legislador que la legislación administrativa resultaba insuficiente. Del mismo modo, no parece que en la actualidad esté todo dicho en esta materia, hasta el punto que el futuro puede deparar el reconocimiento de un bien jurídico relacionado con el uso y abuso de estas nuevas tecnologías.

El panorama actual y ese futuro, a riesgo de que se nos pueda llamar tremendistas, no es el de 1995. Basta consultar datos en la red para percibir un fenómeno cre-

ciente. Pertenecemos a lo que se denomina mundo occidental y conviene por ello tener en cuenta el reciente reconocimiento del Gobierno de Estados Unidos de que aproximadamente 10 millones de norteamericanos son víctimas de fraude electrónico cada año.

O, lo que es más grave, empresas informáticas como McAfee indicaban para 2007 más de 217.000 tipos diferentes de amenazas conocidas y miles más que aún no se han identificado.

En España las estadísticas no son mejores, puesto que las amenazas sobre los sistemas de información han crecido un 55%.

En los últimos meses de 2006 se ha podido constatar un gran flujo de ofertas de programas espía en el mundo de los dispositivos móviles. La mayoría de ellos diseñados para monitorizar números de teléfono y registros de llamadas SMS o para robar mensajes SMS al reenviar una copia a otro teléfono.

Frente a ello se incrementan las medidas de prevención frente a los ataques. Lo demuestra el hecho de que este año el Centro Criptológico Nacional, dependiente del CNI, acaba de incorporar un equipo, cuya principal labor es precisamente detectar los puntos vulnerables y amenazas que puedan afectar a los sistemas de información de las Administraciones públicas y, en caso de ataque concreto, dar un soporte práctico que permita minimizar el posible daño a la red de la Administración central, Comunidad autónoma o Ayuntamiento.

O, del mismo modo, la mayor parte de las empresas de cierta entidad, o bien presentan departamentos de informática que hacen especial hincapié en la seguridad, o caso contrario acuden a empresas externas. Pero también es de conocimiento público que, dada la situación actual, para muchas empresas resulta más sencillo absorber los costes del delito, aumentando los gastos en seguridad de sus redes, que buscar y procurar que haya una intervención penal. Hasta el punto de que, a veces, los accesos no autorizados se ocultan a la mayor parte de los usuarios o incluso directivos de la empresa, quedándose en los especialistas o encargados de seguridad, de forma que sólo en los casos de daños irreparables la conciencia se agudiza.

Esta realidad puede desarrollar y potenciar el reconocimiento de un nuevo grupo de delitos autónomos en el Código Penal, que tengan en cuenta principios nuevos, una suerte de seguridad o de privacidad informática o de otro modo, pero que no dependan en su interpretación del ámbito patrimonial o de la intimidad o cualesquiera otros bienes jurídicos tradicionales. Nuevo grupo que dé cobertura a supuestos reprochables que hoy quedan impunes, sin perjuicio de la protección actualmente dispensada a otros derechos, que en su caso daría lugar a la aplicación de reglas de especialidad o en general de concurso de delitos.

No hay que llegar a extremos como los de quienes afirman la existencia de domicilio informático, pero sí admitir que se necesita protección de nuestra privacidad informática, sin necesidad de acudir al título genérico de la intimidad y privacidad actual. Ello, sin perjuicio de admitir que cualquier innovación en este sentido, o los tipos penales relacionados con la protección de ese hipotético bien jurídico novedoso, deben tener elementos o conceptos correctores, de modo que sea exigible al usuario una política de seguridad mínima de protocolos, uso de contraseñas, control de acce-

sos... Política de seguridad de unas determinadas características en empresas o administraciones, pero igualmente exigible, aunque de menor entidad, en el usuario particular, sobre todo cuando éste se encuentra conectado a la Red.

En todo caso, y para cerrar este apartado, buena muestra de que los delitos informáticos cobran importancia en nuestro trabajo diario (cuando menos en el de los Fiscales, que finalmente repercutirá en los Juzgados) es que, después de varios años de hacer hincapié sobre el incremento y las dificultades de respuesta en este tipo de delitos, en sucesivas Memorias de la Fiscalía General, este mismo año, el Fiscal General del Estado, ha incidido de forma especial, en la materia, dictando un Decreto novedoso, dentro de la línea iniciada por la Instrucción 11/2005, de dar un tratamiento unitario y de mayor eficacia a determinadas materias. Por esta razón, en los últimos meses, se han venido nombrando Fiscales de Sala, como Delegados del Fiscal General y coordinadores en materia de medio ambiente, seguridad vial, y otros bienes jurídicos de especial relevancia. La nueva inclusión de un Fiscal Delegado en materia informática puede suponer un reconocimiento implícito de la necesidad de dar un tratamiento unitario a los diferentes tipos penales.

Este nuevo Decreto del Fiscal General, indica que *... la modernización de la sociedad actual se caracteriza entre otros aspectos por el incesante auge de las nuevas tecnologías cuya influencia en la vida cotidiana de los ciudadanos aumento diariamente….. destacando el uso de la informática en general y de internet en particular. Su generalización ha tenido también el lógico reflejo en la actividad delictiva, de forma que, de una parte, van apareciendo nuevas formas de criminalidad antes impensables, y, de otra, los viejos tipos penales se ven remozados con nuevas y ocurrentes formas comitivas, que exigen un tratamiento propio y especializado.*

La misión concreta de este Fiscal de Sala es asumir la coordinación de los delitos cometidos específicamente a través de medios informáticos y singularmente por medio de internet, a fin de asegurar un tratamiento unitario y la uniformidad de los criterios de actuación, ejerciendo la dirección de quienes en la Carrera Fiscal, lleven estas materias. Para ello, impartirá las instrucciones oportunas, estableciendo relación con las unidades judiciales especializadas y cualesquiera otras funciones necesarias para la finalidad indicada.

Siendo como es importante el reconocimiento de una nueva especialidad, hemos de esperar al próximo Código Penal como referente del contenido exacto de la misma, puesto que, en principio, el que fija el Decreto (delitos cometidos específicamente a través de medios informáticos y singularmente por medio de Internet), abarca un número excesivo de tipos penales y resulta de difícil cometido para las posibilidades de las Fiscalías, siempre escasas en medios materiales y personales.

IV. DIFICULTADES EN LA INVESTIGACIÓN Y PRUEBA DE ESTOS DELITOS

El primer paso que se da al asumir una investigación es el examen de competencia. Y en este aspecto, aunque es un problema extendido a muchos otros delitos, lo cierto es que los criterios no son uniformes, más en esta materia donde intervienen máquinas y personas colocados en muy diferentes lugares, lo que da lugar a remisiones de causas que dilatan en el tiempo la tramitación.

Está relativamente asumido que en los próximos años, con los nuevos productos informáticos que se van a ofrecer, tendremos un abanico de formas lesivas tan amplio que dejarán el sabotaje de ordenadores o los aumentos ficticios de cuentas, en figuras arcaicas. Productos y acciones que no pueden ser abordados desde una única perspectiva territorial. Problema que se incrementa si incluimos lo que algunos autores han comenzado a llamar paraísos informáticos, que tienen los inconvenientes de los paraísos fiscales, incrementados por el dato de que pueden ser usados mucho más fácilmente que los fiscales, que requieren determinados niveles económicos o de asesoría.

Fijada la competencia, las diligencias a practicar para acreditar el delito, que posteriormente puedan tener posibilidad de convertirse en prueba suficiente para una sentencia condenatoria, son variadas. Analizaremos sólo algunas de ellas, en cuanto que en esta materia pueden ofrecer peculiaridades.

Medidas restrictivas de derechos.- Es importante el hecho de que el Tribunal Constitucional reconozca su posibilidad en esta materia (entrada y registro, intervención telefónica), posibilidad muy discutida, y que planteaba serias dudas a los Jueces de Instrucción, acostumbrados a adoptar dichas medidas en otro tipo de materias.

Con relación a una intervención telefónica, el Tribunal Constitucional se ha pronunciado recientemente en sentencia 104/06 de tres de abril de este año. El caso partía de una investigación que había realizado la policía judicial de Barcelona, en concreto el grupo de delitos relacionados con la informática y la ciberdelincuencia, investigación iniciada por noticias anónimas que les habían llevado a páginas web en las que se ofrecían productos informáticos no autorizados. El caso dio lugar a condena por delito contra la propiedad intelectual y de revelación de secretos. La defensa llego hasta el Tribunal Constitucional, con varios motivos de impugnación, entre ellos, precisamente el de que la medida de interceptación telefónica era desproporcionada con relación a la pena que corresponde a estos los tipos penales. Todos sabemos que las medidas limitativas exigen motivación y sobre todo proporcionalidad. Partiendo de esta premisa, el Tribunal Constitucional ha ratificado la legitimidad de la restricción en estos supuestos y da argumentos, ciertamente importantes, para todos los delitos informáticos en general.

El primero de ellos es la transcendencia y la repercusión social de estos supuestos, puesto que para acordar estas medidas hay que atender a la gravedad del hecho, más que a la gravedad de la pena que lleve aparejada el hecho. Y el segundo, y más importante, que esas conductas penadas, estaban relacionadas con el USO Y ABUSO DE LAS NUEVAS TECNOLOGÍAS, las cuales, a mayor abundamiento, suelen ser susceptibles de generar mayores perjuicios económicos. Menciona el TC la potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito, potencialidad lesiva que se manifiesta en que

– la tecnología informática facilita la comisión de delitos,
– y, sobre todo, suelen ser infracciones de mucha mayor dificultad de persecución por las vías usuales de investigación.

Extremos éstos que vuelven a incidir en realidad, en uno de los grandes problemas actuales de estos delitos, cual es que ya no estamos, como al principio, ante tipos penales con un número de posibles autores reducido, al quedar reservados para especialistas, sino que la mayor parte de las posibilidades de ataque se encuentra al alcance de cualquiera.

Testigos y peritos.- Utilizamos para los delitos tradicionales conceptos que manejamos habitualmente o con los que nos familiarizamos a lo largo de nuestra experiencia profesional. Con este tipo de delitos, encontramos un lenguaje extraño, plagado de anglicismos, en el que el mismo tipo de preguntas que se han de realizar en la fase de instrucción o el juicio oral, exige una formación, o cuando menos preparación del caso, superior a la de los supuestos habituales de robos, homicidios... Es por ello relativamente necesario acudir a las periciales.

En otros delitos, el Juzgado o la Fiscalía cuentan por ejemplo con los médicos forenses, con preparación ad hoc para la función que desarrollan, y el ámbito en que se mueven. En el ámbito económico, es frecuente acudir al deber de colaboración de las Administraciones Tributarias con los órganos jurisdiccionales y con la Fiscalía, no sólo para obtener peritos, sino sobre todo, para desarrollar adecuadamente las líneas de investigación, a veces complicadas desde meros conocimientos jurídicos, practicando los funcionarios designados en auxilio las diligencias que fueran necesarias bajo la supervisión del Juzgado o de la Fiscalía.

Parece lógico, pues, que en los delitos informáticos es igualmente importante contar por un lado con ese auxilio en la investigación y, por otro, con informes periciales, susceptibles de ser llevados al juicio oral. Sin embargo, las unidades de policía especializadas son escasas y no suficientemente desplegadas en todas las zonas; no siempre cuentan con titulados informáticos, lo que es utilizado por las defensas, para intentar minusvalorar sus conclusiones, partiendo de que por su parte acuden a titulados informáticos del sector privado. Esto no siempre plantea excesivos problemas, en la medida que un informático suele acudir a los ordenadores desde una perspectiva de comprender y hacer funcionar la máquina, mientras que el investigador en estos delitos debe ir a buscar y asegurar los datos que incriminen, esto es, que acrediten el hecho y el posible autor, misión ésta para la que dichas unidades suelen estar preparadas.

Tanto en los casos de estos funcionarios policiales que auxilian en la investigación, como en el de los testigos, personal de una empresa que han experimentado el ataque informático, la figura procesal del testigo, resulta insuficiente.

En puridad, los testigos narran sólo los hechos que perciben, y serían los peritos quienes nos deben explicar las complejidades técnicas, pero en estos casos lo deseable es que los testigos puedan completar y aportar datos sobre los hechos desde sus propios conocimientos. Resulta, por tanto, totalmente recomendable acudir a una nueva figura de carácter procesal civil, creada en la nueva Ley de Enjuiciamiento Civil, el testigo-perito, que en ocasiones puede llevar a que no necesitemos ni siquiera peritos, cuyo nombramiento, realización de informe, aclaraciones al mismo y otros trámites, lo único que logran es ralentizar el procedimiento. En la medida que la Ley de Enjuiciamiento Civil es de aplicación supletoria a la LECrim, puede ser muy útil pedir este tipo de declaraciones.

Es curiosa, finalmente, la discordancia doctrina-jurisprudencia que se manifiesta en esta materia. La práctica nos demuestra que la redacción de los tipos penales actuales es muy insatisfactoria y origina problemas que se alargan en el tiempo, sin solución práctica, y con conductas claramente reprochables que quedan impunes. Cuestiones aparentemente sencillas, como calificar la utilización de un servicio informático, como equivalente a la transferencia de un activo patrimonial, son negadas, por lo que quizá,

a diferencia de lo que se podía mantener hace unos años, sería deseable una simplificación de los tipos penales, en un apartado propio, que incluyera diferentes artículos o capítulos, en los que encuadrar, por un lado, la obtención indebida de prestaciones utilizando medios informáticos, por otro, los ataques a los sistemas o programas informáticos como violación de la privacidad informática o con resultado dañoso y, finalmente, los ataques a cualesquiera otros bienes jurídicos. Tipo penal este último, específico, que se puede reconducir a los tipos básicos, de forma similar al artículo 438 CP que, dentro de los delitos contra la Administración Pública, recoge la apropiación indebida y la estafa cometida por funcionarios públicos. Y así como dicha mención específica se realiza por el abuso de cargo por parte de aquél, en este caso, este tipo o tipos pudiera tener su sentido o justificación, en la mayor facilidad que prestan las nuevas tecnologías, no sólo para la comisión del delito, para la ocultación y encubrimiento del mismo, sino también el mayor riesgo o potencialidad lesiva a que en determinados supuestos pueden dar lugar.

Pero este último párrafo, como es lógico y todos podemos entender, es incluido como final, sólo en la medida en que quienes aplicamos el derecho queremos mayor simplicidad, lo cual, también ha de reconocerse, no siempre resulta de correcta técnica jurídica.