Los Delitos Informáticos en el Derecho Español

MIGUEL GÓMEZ PERALS
Profesor en la Facultad de Derecho y en la Escuela Universitaria de Empresariales de la Universidad de la Laguna.
(ESPAÑA)

SUMARIO

INTRODUCCION

En las postrimerías del siglo XX en que nos encontramos se produce el tránsito de la llamada «era de la imprenta» a la de la «informática». La irrupción de esta novedad tecnológica plantea enormes posibilidades a la vez que serios problemas jurídicos. Y ello porque los avances técnicos son sus-

ceptibles de utilizarse no sólo como instrumentos de progreso humano sino de dominación y explotación de los hombres entre sí.

Aunque sería prolijo enumerar las ventajas que conlleva la Cibernética, destaquemos la simplificación y economía que supone la automatización de múltiples operaciones mecánicas –antes desarrolladas manualmente– la celeridad y el aumento de la eficacia de los servicios informatizados.

Por contra, se ha criticado, la aparición de ciertos fenómenos indeseables como el aumento del paro y la propia delincuencia informática. Baste a estos efectos recordar la polémica sobre la bondad o maldad moral de la energía nuclear, en principio aséptica como tal fenómeno científico. Pero como desgraciadamente el progreso técnico no avanza parejo con el desarrollo moral del hombre, a cada adelanto tecnológico le acompaña una específica picaresca cuando no una auténtica morfología delictiva como es el caso de la delincuencia informatica.

Aceptada la interdependencia entre el nivel de evolución tecnológica, el grado de desarrollo económico y social y las manifestaciones criminales, nos adentraremos en el estudio de la delincuencia informática.

CONCEPTO

A pesar de que no existe unanimidad en la doctrina, respecto a qué se entiende por Delincuencia Informática, es preciso el establecimiento de alguna definición –por perfectible que sea– para poder delimitar el objeto de nuestro estudio.

Así, con criterio ecléctico y amplio podemos conceptuarla como el conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto –doble vertiente que después examinaremos– a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos. O centrándonos más en el aspecto patrimonial: el conjunto de acciones dolosas que provoca un perjuicio a personas físicas o entidades, sin que sea necesario que ello conlleve un beneficio material para su autor, o viceversa, produce un beneficio ilícito para su autor aun cuando no perjudique de forma ostensible a la víctima.

Hemos de hacer sin embargo una precisión terminológica: la expresión «delitos informáticos» es utilizada en este estudio en un sentido impropio, pues no existiendo legislación que tipifique todavía estos supuestos, no puede hablarse de auténtico delito.

El ámbito de incidencia de la Delincuencia Informática, o dicho de otro modo los bienes jurídicos que constituyen su objetivo son cada vez mas variados: la esfera privada de la personalidad del ciudadano –lo que los anglosajones denominan «privacy»–, y su esfera patrimonial: campos ambos a que

nos referiremos en este comentario. Ello sin perjuicio de que en otras ocasiones las conductas afectan intereses públicos (seguridad del Estado, datos administrativos, etc.)

Más concretamente la intimidad y dignidad de la persona física, se ven lesionadas cuando datos relativos a los aspectos más variados de su existencia (profesionales, económicos, sanitarios,) son almacenados, consultados, transmitidos y utilizados no siempre para los fines que justificaron la creación del fichero en cuestión, o por personas diferentes de las autorizadas para ello.

Por otra parte, el segundo bloque de bienes jurídicos afectados por esta forma de criminalidad son los patrimoniales en sentido estricto, referidos a los derechos e intereses económicos y financieros (cuentas corrientes, percepciones por dividendos o pensiones, etc).

CARACTERES

Respecto de su encuadre doctrinal ya hemos dicho que la Delincuencia Informática puede considerarse como una sección de la llamada «delincuencia económica»; para algunos autores incluso un subgrupo de la de «guante blanco.» Aunque ello no es siempre exacto dado la pluralidad de bienes jurídicos que pueden ser afectados, sí resulta cierto de los supuestos cometidos mediante medios informáticos de los cuales vamos a comentar sus principales rasgos por ofrecer mayor interes que los casos en que dichos medios informáticos constituyen el objeto material de la acción.

Para determinar los principales rasgos que permitirían construir una categoría con los dispersos delitos informáticos es preciso atender tanto al sistema económico y al contexto social en que tienen lugar, como a las propias características tecnológicas de la Ciencia Informática.

Una nota sociológica interesante de la Delincuencia Informática es la escasa publicidad que se le da por la víctima, principalmente entidades bancarias, para no provocar su desprestigio y la desconfianza de sus clientes. El porcentaje de las llamadas «cifras negras» en esta delincuencia es muy alto. Los delitos son descubiertos generalmente por denuncias anónimas o simple casualidad. Las informaciones verbales son inoperantes no sólo por la falta de pruebas contra el presunto autor sino por la virulenta reacción de éste para evitar su deshonra provocada por la acusación.

Desde el aspecto económico, la «rentabilidad» de estos delitos se calcula que es una tercera parte superior a la de cualquier otro tipo, ya se trate de una o pocas ocasiones en que se sustraen grandes cantidades o de infinidad de operaciones por un importe mínimo (técnica del salami). La lesividad de estas acciones se acentúa porque hoy en día la interconexión entre las actividades económicas genera un efecto de «cascada» en que se ven afectadas multitud de entidades, por lo que el perjuicio aumenta considerablemente.

Por ello resulta especialmente difícil la cuantificación de este perjuicio, pero desde luego suele existir una gran desproporción.

Desde el punto de vista técnico son rasgos decisivos el cáracter incorporal de algunos elementos de la Informática (software), la posibilidad de acumular un ingente caudal de datos en volúmenes reducidísimos (bases de datos), la práctica desaparición del factor distancia o espacio (gracias a las redes de comunicaciones), la reducción alucinante del factor tiempo en la realización de cálculos y procesos complejos. La posibilidad de alterar programas y datos sin dejar rastro dificulta enormemente el hallazgo de pruebas. La complejidad técnica de la materia reduce su conocimiento a un circulo reducido de expertos, respecto de los cuales también resultarían inútiles los controles del sistema. Respecto de esto último nos podríamos plantear el eterno problema: ¿Quién controla al controlador?.

Un rasgo común a estas figuras desde el punto de vista de su punición es la posible consideración de la multa impuesta por el fraude –en los supuestos cometidos mediante medios informáticos– como uno más de los gastos de explotación, por lo que la función preventiva debe actuar también a través de efectivas medidas de seguridad.

La creciente interconexión y trasmisión interfronteriza de datos ha puesto de manifiesto como este fenómeno afecta de modo semejante a los países de un mismo entorno tecnológico.

La internacionalización del problema hace cada vez más necesaria la cooperación interestatal tanto administrativa como judicial para la investigación y prueba de estos delitos. Existen ya trabajos como la Recomendación del Consejo de Europa R (81) 12, a cargo de los Profesores BOLLE y TIEDEMANN, que reflejan la creciente preocupación supranacional por el tema.

SUJETOS ACTIVO Y PASIVO

Respecto del sujeto activo nos centraremos en los posibles autores:

–Los operadores, programadores u otros sujetos en legítima relación con la elaboración del programa. Las personas autorizadas actuan ilícitamente cuando se extralimitan.

–Cualquier persona a través de terminales publicas o interceptando líneas de transmisión de datos a distancia, o bien causando daños a los medios informáticos, ya sean empleados descontentos o activistas con móviles políticos o ideológicos. Son terceros o extraños.

–Los titulares legítimos del sistema, por título de propiedad y por cualquier otro título que les habilite para el disfrute de dicho sistema informático. Resulta curioso cómo la utilización ilícita por los titulares suele ser medio de comisión de otros delitos como el alzamiento de bienes mediante la crea-

ción de doble contabilidad. En este apartado incluiríamos la inutilización de programas por su propietario cuando se dan determinadas circunstancias.

El retrato robot del delincuente informático seria el de un varón, relativamente joven, profesional competente en técnica informática o bien antiguo empleado o usuario que por su trabajo o por la confianza que la empresa ha depositado en él, tiene acceso al sistema informático y conoce sus deficiencias.

También puede ocurrir que el delito se comete por persona jurídica a través de sus órganos. Orillemos la polémica cuestión de la responsabilidad penal de esta clase de personas que es diferente de la de las personas físicas ejecutoras de la acción y de su responsabilidad civil subsidiaria. Y mencionemos sólo algunas medidas punitivas que pueden imponerse: desde la advertencia o caución de buena conducta, confiscación de ganancias obtenidas, prohibición de ejercer determinadas actividades relacionadas con la informática, prohibición de obtener beneficios de naturaleza pública, hasta su cierre.

En cuanto al sujeto pasivo comprende tanto los titulares y demás beneficiarios legítimos del sistema, como los usuarios y terceros de buena fe. La fisonomía típica de la víctima informática es la de una empresa con escaso o nulo nivel de seguridad informática, en que se procesan transacciones que suponen movimientos de fondos y con personal descontento.

SUPUESTOS DE DELINCUENCIA INFORMATICA

Dada la variedad de estos supuestos, es imprescindible su clasificación para su estudio con un mínimo de rigor científico. A su vez, esta clasificación puede hacerse siguiendo diversos criterios.

Uno de ellos es el de atender a la función que el sistema informático –sus elementos o procedimientos– desempeñan en dichos delitos informáticos: el de objeto material de la conducta o el del instrumento que auxilia la acción típica. Así se distinguen dos grupos: los ilícitos patrimoniales contra elementos informáticos y aquellos otros cometidos por medio de procedimientos informáticos. Con independencia de esta distinción surge otra: la que diferencia –respecto al sistema informático– aquellas conductas que afectan a los elementos materiales o «hardware» de aquellas otras que se relacionan con el material lógico o software.

Ilícito contra elementos del hardware informático.

Podríamos citar el hurto, robo o apropiación indebida de un ordenador, incluso su inutilización o destrucción, figuras todas ellas a las que se podrían aplicar perfectamente las reglas propias de los elementos ordinarios no informáticos. Especial interés en temas informáticos presenta el llamado hurto de «tiempo–máquina» que la doctrina considera atípico como tal hurto de uso,

por lo que de momento sólo cabría la reclamación por vía civil de la correspondiente indemnización.

La destrucción, menoscabo o inutilización del hardware podría reconducirse a los delitos de incendio (547 y ss. del Código Penal), estragos (554 y ss.) y daños (557 y ss.) supuestos estos que se diferencian por su respectivo medio comisivo, siendoles común por el contrario la falta de un ánimo –por lo menos inmediato– de enriquecimiento y la intención de causar un perjuicio patrimonial.[1] Respecto de los daños es interesante la circunstancia de una inutilización o pérdida de su operatividad original sin implicar necesariamente destrucción física o pérdida de su sustancia, por lo que queda demostrado una vez más que el detrimento de valor económico de un bien puede recaer sobre la sustancia material o sobre la funcionalidad de su uso. Todo ello sin perjuicio de la tipificación de estas conductas como delito o falta dependiendo de las cuantías previstas en el Código.

Ilícito contra el software informático

La acción recae sobre la información o conjunto de datos almacenados en el diskette o memoria, sin que resulte alterado físicamente ninguno de los elementos del Hardware, o por lo menos sin que sea necesaria dicha alteración física, aunque pueda concurrir. La doctrina distingue varios supuestos:

–El «apoderamiento» de ficheros informáticos (copia con simultánea destrucción del original), hipótesis esta que plantea el siguiente problema. Aceptemos el concepto de cosa corporal mueble como todo objeto mueble o inmueble, aprehensible, susceptible de fundamentar un derecho real de propiedad y valuable en dinero. Este concepto sera coherente con la idea de «tomar o apoderarse» en que se basa la idea clásica de apoderamiento. Pero no parece aplicable a los elementos lógicos o software, salvo que el tipo se configure como desplazamiento patrimonial y no material.

Y ello porque el software está caracterizado como antes dijimos por su inmaterialidad; es en realidad una especie de flujo electro-magnético, por lo que su protección penal podrá asimilarse a la del flujo de energía–eléctrica en los arts 536 y ss. del Código Penal. Sin embargo, esta tesis de las defraudaciones es criticable puesto que en los programas informáticos la relevancia corresponde al contenido de instrucciones y datos y no al consumo ilícito de flujo de energía, que actúa sólo como vehículo de aquel contenido.

Pero si bien los ficheros informáticos no parecen susceptibles por sí mismos del delito del apoderamiento clásico, sí que lo podrían ser cuando el delincuente se apodera del soporte físico que contiene aquel fichero.

Tampoco la estafa encaja bien en estos supuestos. Y no tanto por aquella objeción del concepto de cosa corporal sino por no admitirse que el engaño

[1] Para un análisis más detenido de la posible aplicación de estos tipos a las acciones informáticas, vid. ROMEO CASABONA, «Los delitos de daños en el ámbito informático». Cuadernos de Política Criminal, núm. 43, Madrid 1991, págs. 97 y ss.

–requisito imprescindible en ese delito– pueda darse con respecto a una máquina, en este caso el ordenador. Algun autor considera que esta objeción es artificial: el engañado sería el sujeto titular de dichos objetos.

–Copia sin destrucción del original, supuestos de acceso a la información que la doctrina relaciona con las siguientes figuras:

a) Descubrimiento y revelación de secretos (Arts 497 a 499 a.i.) comprendiéndose tanto los supuestos en que el apoderamiento de papeles o cartas tiene lugar para descubrir secretos como también para obtener un lucro; por persona autorizada (en el caso especial de tratarse de funcionario público véase arts 367 y 368) o no autorizada. Aquí se plantea el problema de interpretación doctrinal de si la expresión «papeles o cartas» puede comprender los ficheros informáticos, como en efecto parece coherente con el actual tratamiento de fotografías y cintas magnetofónicas como medio de prueba.

b) Competencia ilícita, regulada en la antigua Ley de 1902 y en la actual de 1989.

c) Propiedad intelectual, regulada en la antigua Ley de 1879 y la actual de Ley 22/1987 de 11 de Noviembre, así como en la Ley Orgánica de Modificación del Código Penal 6/1987 de igual fecha que retoca los arts. 534 y ss. de este cuerpo legal. El paradigma sería el «pirateo» de un programa.

Completando a los anteriores, el supuesto de copia de un fichero en papel que se puede configurar, si se desprecia el valor del papel utilizado, como un hurto por el valor del fichero.

–Destrucción o inutilización de ficheros; sin embargo el delito de incendio afectaría a los elementos físicos, por lo que parece mas apropiado el delito de daños para proteger el software en sí. Considera Romeo Casabona en el artículo citado [2] que nuestro Código no exige la corporeidad del objeto dañado, precisamente porque la acción de dañar no supone la traslación de un patrimonio a otro, como sería típico de los delitos llamados por ello de enriquecimiento. Por el contrario, el art. 557 del Código Penal solo se refiere a dos notas: que se trate de un objeto de propiedad ajena y que el supuesto no esté comprendido en los delitos de incendio y estragos.

Romeo Casabona resuelve varias cuestiones a cuyo análisis nos remitimos. Baste mencionar que respecto del tipo objetivo se admite la conducta omisiva y en cuanto al tipo subjetivo, lo más frecuente es la exigencia de dolo. Otro aspecto sería la delimitación entre actos preparatorios, tentativa y consumación [3].

La consumación en el delito de daños se determina por la producción efectiva de la destrucción o inutilización, admitiéndose las formas imperfectas de ejecución. Quizá el ejemplo más práctico sea determinar si la introduc-

[2] Op. cit. págs. 104 y 105.
[3] Op. cit. págs. 109 y 110.

ción de una rutina destructiva en el programa constituye un acto ejecutivo punible (tentativa) o uno preparatorio impune.

Parece que la cuestión estriba en que el autor conozca el cuándo y el sí de la activación del mecanismo. Si conoce si se va a producir la activación del mecanismo destructor aunque no sepa cuándo –a fortiori si lo sabe– estaremos ya ante actos ejecutivos; si el resultado no se llega a producir por descubrimiento por el potencial perjudicado, apreciaremos tentativa.

En cambio si el autor conoce el cuándo pero no el sí porque esto depende de un evento ajeno (actuaciones de terceros) estaremos ante actos preparatorios impunes –con mayor razón si ni siquiera conoce el cuándo–. Desde que se produzca dicho evento, es decir, se conozca el sí, empieza el peligro para el bien jurídico pudiéndose y la fase de tentativa pudiéndose dar también el desistimiento hasta terminar en la consumación.

Claro está que si se conservaran copias de seguridad idénticas a las destruidas, el delito habría que apreciarlo en grado de tentativa.

Otro tema interesante que ya apuntábamos al hablar de la autoría es el de la inutilización del programa de ordenador por el titular de los derecho de explotación. [4] El caso más frecuente es el de la empresa comercializadora de software que introduce en los programas vendidos o cedidos rutinas que operarán ante ciertas circunstancias como la falta de pago o la reproducción no autorizada del programa en cuestión. El primer escollo que encontramos para encajar este supuesto en el tipo de daños es que nuestro Código exige la ajeneidad de la cosa objeto del delito, salvo el caso del 562 relativo a daño en cosa propia de utilidad social o economía nacional. Y en el ejemplo citado los derechos de explotación, sino la propiedad intelectual, permanecen, salvo pacto, en la empresa suministradora, obteniendo el cliente sólo el derecho de uso. Los que consideran que no es aplicable el tipo de daños, piensan que la cuestión quedará relegada al ámbito civil por incumplimiento de las respectivas obligaciones contractuales. Otros creen que si bien no son propiedad del cliente de aquellas empresas las instrucciones del programa, sí lo son los datos con él procesados y que por lo menos en cuanto a éstos sí sería aplicable el tipo de daños.

También se ha planteado si sería alegable por dichas empresas la eximente de legítima defensa para justificar aquella introducción de rutinas destructivas. Parece que el impago por el cliente no tendría la consideración de agresión ilegítima y por tanto no sería aplicable tal eximente. Respecto de la otra circunstancia la reproducción no autorizada del programa cedido, si bien constituye una agresión ilegítima, típico supuesto de derecho de autor, lo cierto es que sólo parcialmente procede la aplicación de la eximente por la razón de que en el estado actual de la técnica no parece necesario racional-

[4] Op. cit. págs. 111 y 112.

mente el medio empleado –la destrucción de los datos– para impedirla o repeler dicha copia.

Los ilícitos patrimoniales realizados «por medio» de sistemas informáticos.[5] Su auge se debe a la creciente informatización de las operaciones comerciales, bancarias y bursátiles, fenómeno llamado Transferencia Electrónica de Fondos. Las conductas más características en este ámbito son defraudaciones que se cometen mediante la introducción de datos falsos o la alteración de programas para determinar la transferencia automática, ingreso, o reconocimiento de créditos en favor del autor. Un caso típico sería el pago de pensiones a favor de personas en realidad fallecidas ya, o el redondeo de céntimos en las nóminas o intereses en favor de una cuenta del autor.

Podría reproducirse aquí lo dicho antes respecto de la consideración de cosa corporal imprescindible para la configuración del apoderamiento. Y ello porque la «moneda escritural o moneda de giro» no es una cosa mueble, sino sólo representación de una deuda de valor generada por el traspaso de un crédito de una cuenta corriente a otra, mediante un asiento contable.

Otro elemento del fraude informático sería el perjuicio causado que puede ser económico (dinero, mercancías, valores negociables, servicios) de fácil cuantificación; o inmaterial (prestigio) de mas difícil determinación cuantitativa.

Aún admitiendo este «hurto bancario» habría que considerar que el momento de su consumación es el de la práctica del asiento contable y no en el de la extracción a través de la cual el autor se apodere del dinero físico. Y ello porque ya desde el primero de estos dos momentos el sujeto activo tiene la disponibilidad de la «cosa».

Otro argumento para calificar esta figura de hurto y no de estafa es que así califica la doctrina las maniobras físicas de astucia sobre las cosas, pues a las máquinas no se les puede engañar. Y ello contando con la existencia de perjuicio patrimonial.

También merece examinarse el supuesto de falsificación de documento privado con perjuicio de tercero o con ánimo de causárselo (306 C.P). La objeción en este caso sería la de considerar «documento» los datos recogidos en un soporte informático (diskette, por ejemplo) porque no serían directamente legibles por el hombre.

No puede faltar una somera referencia al tema de los abusos perpetrados en los «cajeros automáticos». Según sea el supuesto de hecho la calificación penal difiere. Distingamos básicamente si la extracción la realiza el titular de la tarjeta o un extraño.

---

[5] González Rus Juan José, «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos». Poder Judicial. Número Especial IX, págs. 48 y ss.

Así, en las extracciones repetidas en un mismo día por el titular de la tarjeta, sin superar el saldo disponible en su cuenta corriente, sólo parece haber incumplimiento contractual del cliente con respecto al Banco o Entidad, que podría sancionarse por éste con la retirada de la tarjeta.

Pero incluso superando el saldo disponible no aparece tampoco la responsabilidad penal derivada de hurto o estafa, si es que nos decidiéramos por la admisión de esta última figura a pesar de la objeción doctrinal reseñada. El cajero entrega la cantidad porque ha sido programado para ello: no hay voluntad contraria de la entidad. Sin embargo, si el titular utilizase una tarjeta anulada o caducada, estaríamos ante un hurto; en grado de tentativa si el cajero retuviese la tarjeta.

Si la extracción es realizada por un tercero con tarjeta perdida o sustraída pueden apreciarse diversas figuras penales. Si la tarjeta fue encontrada y no devuelta, apropiación indebida; si fue sustraída, hurto; si se obtuvo mediante engaño, estafa; en todos los casos por el importe de la tarjeta en sí. Si se la quiere para usarla y devolverla después, estaríamos ante esas mismas infracciones en su modalidad de uso, que son atípicas. También se ha discutido si podría apreciarse el delito de robo con fuerza en las cosas, puesto que la tarjeta cumple el papel de «llave» y las legítimas sustraídas al propietario tienen la consideración de falsas. Pero esa tesis es rechazada por aquellos que consideran que la banda magnética no tiene el carácter corporal de las genuinas llaves.

Otro caso interesante es la utilización de tarjeta falseada o manipulada.- Para algunos podría incluirse entre las falsificaciones de documentos mercantiles del art. 303 C.P.; otros niegan el carácter de documento a la anotación magnética por no ser legible directamente por el ser humano.

MEDIOS COMISIVOS

En el epígrafe anterior hemos clasificado las figuras –todavía no auténticos tipos por no haberse positivado– más frecuentes que podrían constituir la llamada Delincuencia Informática. Veremos aquí las principales conductas que conforman la acción básica en cada una de aquellas figuras.

-Manipulación. Consiste en la supresión o borrado, modificación, ocultación, cambio de lugar de datos o en la introducción de otros falsos, o bien en la alteración de las instrucciones que constituyen el programa. Según el momento en que se produzca estaremos ante una manipulación previa u operada sobre el input o instrucciones internas del programa; simultánea a la ejecución del programa; y posterior a la misma o realizada sobre el output o datos de salida.

The quick brown fox jumps over the lazy dog. Now is the time for all men. Las manipulaciones en las dos primeras fases indicadas son más peligrosas que en la tercera. Y ello porque una vez programadas estas alteracio-

nes pueden perpetuarse durante el tiempo que se desee (no en vano uno de los rasgos del delito informático es su continuidad) e incluso puede programarse la propia autocancelación de la manipulación operada una vez transcurrido determinado plazo lo que borraría cualquier pista de ella.

-Espionaje. Agrupa actividades de obtención no autorizada de datos o programas, o bien de divulgación de los obtenidos legítimamente. Su motivación puede ser fundamentalmente comercial, industrial o militar.

-Sabotaje. Referido a conductas que persiguen la destrucción o incapacitación de los sistemas informáticos o de alguno de sus elementos (hardware y software), con la consiguiente paralización de actividades empresariales o administrativas que ello conlleva.

Tanto el espionaje como el sabotaje son técnicas utilizadas principalmente por organizaciones terroristas en sus atentados contra medios informáticos. Como casos más curiosos recordemos el ya extinto grupo CLORO, Comité para la Liquidación o Conversión de los Ordenadores, que se autoproclamaban trabajadores de la Informática a la que consideraban un instrumento de dominación para el control y represión del pueblo. Otras organizaciones pretendidamente «pacifistas» dirigieron su violencia contra sistemas informáticos al servicio de instalaciones militares como la OTAN, o simplemente civiles, como la central telefónica de Ríos Rosas en Madrid.

COMISION, PERSECUCION Y PREVENCION

Un factor que contribuye en gran medida a la comision de delitos informáticos es el hecho de que la mecanización que supone la informática no se haya compensado con el establecimiento de los oportunos controles informáticos y contables. Estos controles sustituirían a los que antes de dicha mecanización se efectuaban manualmente. Después nos referiremos a la llamada seguridad informática, como vía de prevencion de esta forma delictiva.

Son factores que dificultan la persecución de estos delitos la falta de una legislación específica y la escasa preparación los Cuerpos de Seguridad del Estado en materia informática. Recordemos a este respecto que en EEUU se ha creado recientemente la llamada Policía Informática para la investigación y obtención de pruebas suficientes. El ejemplo nos demuestra cómo el personal investigador ha de reunir conocimientos interdisciplinares en materia infomática, empresarial y jurídico penal.

Además, en la investigación de los delitos informáticos tenemos el «handicap» de que ya la misma averiguación de si el crimen ha sido efectivamente cometido es difícil, mientras que en los tipos clásicos por lo menos este dato suele ser evidente por señales mas o menos patentes, aunque se ignoren otras circunstancias que por ello han de ser objeto de investigación (autoría, móvil, etc).

Pero reunir las pruebas que fundamenten la acusación es sólo el principio del final. Comienza ahora un largo y tortuoso itinerario procesal–penal hasta conseguir una sentencia condenatoria. Baste con pensar que, aun habiendo obtenido, por ejemplo, la cinta que contiene el programa manipulado, será necesario presentar una transcripción impresa de dicho programa, gracias a la intervención de peritos informáticos puesto que ni el notario ni los jueces suelen serlo. Y así en cada trámite en que se exija acreditar la concordancia entre los lenguajes código y fuente del software.

En conclusión, como dice Luis Camacho, experto en seguridad informática, el daño producido por un fraude informático o mejor dicho, el perjuicio, se calcula sumando al importe de lo defraudado, el coste de la investigación, más las ineficacias en el trabajo derivadas de las pérdidas de tiempo y preocupación por el hecho, mas el deterioro de imagen que la publicidad provoca entre los clientes, más el costo de la duda de lo que puede haberse defraudado sin haberse descubierto todavía.

En materia de prevención de esta delincuencia confluyen diversos factores. Uno de ellos es la seguridad de los propios elementos informáticos. Primero se establecieron medidas puramente físicas como servicios de extinción de incendios o sistemas para impedir o detectar el acceso de personas no autorizadas a las instalaciones informáticas.

Más tarde se han comenzado a implantar –todavía en grado insuficiente– medidas de seguridad propiamente informática como controles internos, pistas de auditoría y otras técnicas para evitar la manipulación o sustracción de datos y programas.

Si bien el ideal sería que dichas medidas tuvieran carácter preventivo, disuadiendo de la comisión de estos delitos, en la práctica, por su escasa implantación, muchas veces se adoptan a posteriori de la producción del daño. Finalidad reparatoria tienen las medidas llamadas de «recuperación». Estas pretenden, una vez producida la inutilización en todo o en parte del sistema informático, su reinstalación en un lugar alternativo para la reanudación lo más pronto posible de la actividad empresarial paralizada, minimizando con ello los perjuicios originados.

Otro factor de prevención es el frecuente chequeo del sistema informático para detectar fallos, retrasos, y otras irregularidades, y poderlos subsanar en cuanto antes. De lo contrario se convierten en probables vías de delito.

Pero como en tantas otras cuestiones, en esta de la prevención de la criminalidad informática es preciso combinar el factor técnico con el humano. Por ello junto a las medidas de seguridad antes vistas, es conveniente una buena política de selección y relación con el personal de la empresa de que se trate, y una creciente mentalización de la necesidad de proteger uno de los activos fundamentales en cualquier actividad moderna: los sistemas informáticos.

DERECHO COMPARADO

No puede tenerse una visión con perspectiva de la problemática de la Delincuencia Informática sin tener presente la situacion en los países de nuestro entorno. Tanto la Ley Francesa de 1978, como las Alemanas de 1977 y la de 1986 sobre criminalidad económica establecen un juego de sanciones de diversa naturaleza: penal –multa y privativa de libertad–, administrativa y civil.

Por su parte la Ley Sueca reformada en 1979, contempla supuestos como la creación o explotación de archivos informáticos de datos personales, sin autorización, y sanciones como la declaración de ilegalidad de tales actividades y cierre del banco de datos. También se refiere a la infracción de las instrucciones que la Inspección dicte al conceder las oportunas licencias o a la transacción de datos a otro sistema informático sin las debidas garantías.

TIPICIDAD DE LOS SUPUESTOS DE DELINCUENCIA INFORMATICA

Después de haber examinado la realidad delictiva en el mundo informático hemos de plantearnos si nuestro ordenamiento jurídico está preparado para hacerle frente a dichas situaciones, dotarles de una regulación y resolverlas.

Mas concretamente:

1. ¿Conviene la tipificación de los diversos supuestos de la mal llamada delincuencia informática estudiados? ¿De cuáles?
2. En caso afirmativo ¿podrían englobarse en los tipos penales existentes en nuestro Código o en otras leyes especiales?
3. ¿Es necesario para ello retocar su articulado o incluso crear nuevas figuras?

Para tratar de responder a estos interrogantes hay que partir del principio de intervención mínima según la naturaleza del bien jurídico tutelado, la intensidad del ataque y el contexto social. Pero para que este principio penal cobre verdadero significado, o dicho de otro modo, pueda evitarse una hipertrofia del Derecho Penal, es imprescindible que exista previamente una regulación administrativa de la materia informática.

Es preciso un marco jurídico que defina el ámbito de la actividad cibernética, delimitando los supuestos admitidos de aquellos otros rechazables. Entre estos últimos, sólo aquellos que más radicalmente repugnan a la conciencia social, deben tipificarse. Ese estatuto jurídico administrativo, previo al penal, habría de contener ya medidas de seguridad que fueran eficaces controles con finalidad preventiva de los ilícitos mas graves.

Es preciso, pues, evitar los dos extremos: intervención mínima, sí; pero suficiente. Una vez que se han discernido cuáles son las conductas más mere-

cedoras de sanción penal, debe estudiarse si conforme a la propia técnica penal y a otro principio jurídico básico, el de legalidad, pueden subsumirse en los tipos existentes.

Admitamos que los dos pilares fundamentales en toda disciplina jurídica son la seguridad y la justicia. Veremos cómo el castigo penal de las conductas mas rechazables a través del criterio de la proporcionalidad garantiza la justicia. Fijémonos ahora en el otro pilar: la seguridad jurídica viene representada por el principio de legalidad, que en el campo penal dota de claridad y taxatividad tanto a las conductas prohibidas como a las sanciones impuestas.

También respecto al principio de legalidad penal debe observarse un equilibrio. Por un lado es cierto que una de sus consecuencias lógicas es la prohibición de la analogía contraria al reo, lo cual podría frenar la asimilación de los delitos informáticos a los tipos ya existentes. Pero también es verdad que no se precisa una detalladísima descripción de las acciones típicas, sino que se permite la interpretación extensiva, lo cual facilita la inclusión de las contravenciones informáticas en el Código Penal.

Ocurre además que en multitud de supuestos la intervención de la informática en la comisión del ilícito no altera esencialmente su repercusión lesiva para el perjudicado. Así por ejemplo una falsedad lo seguirá siendo ya se utilice escritura manual, mecanográfica o de otro tipo. Cuando esto ocurra no está justificada la creación de tipos nuevos. Por su parte, sería interesante plantearnos si estas formas de delincuencia se están dejando de detectar y perseguir por motivos ajenos a su actual atipicidad. Pensemos en factores sociológicos como aquella resistencia de la víctima a la publicidad.

La presencia de especificidades en los delitos informáticos como por ejemplo su frecuente carácter continuo, debía resolverse en la Parte General del Código estableciendo un plus punitivo para los delitos cometidos con auxilio o en relación a sistemas informáticos. Además, y aunque ello no sea objeto del presente estudio, esta técnica resultaría muy conveniente respecto de muchas otras materias, como por ejemplo la delincuencia de funcionarios, porque son innumerables los preceptos en que la condición de funcionario se contempla aislada, casuísticamente para matizar determinados supuestos; cuándo sería conveniente que por razones de claridad y economía se regulara globalmente como una circunstancia agravante genérica, con una penalidad especifica.

En conclusión, hoy en día en el Derecho comparado parece existir una dualidad de vías de tipificación de las conductas informáticas: la creación de nuevos tipos y la reinterpretación, incluso teleológica, de los existentes para dar cabida las nuevos supuestos.

La elaboración de tipos específicos o de equivalencia (Alemania, Austria, Portugal) tiene como ventaja la seguridad jurídica y la concreción que supone. Pero junto a ello, el peligro del casuismo que pretendiendo recoger

todos los supuestos pronto implique obsolecencia dado el ritmo del avance tecnológico y la práctica imposibilidad de comprensión de todas las hipótesis. Si no gozan estos nuevos tipos de la suficiente elaboración doctrinal no sólo no resolverán las cuestiones para las que se suponen que fueron creados, sino que contribuirán al surgimiento de nuevos problemas.

La interpretación de los tipos existentes es precisa para la adecuada matización del bien jurídico, el objeto material y las modalidades comisivas, entre otros factores. Con ello se completarían los tipos existentes actualizándolos pero sin crear tipos autónomos. También se mejoraría su técnica corrigiendo cuestiones como la determinación de la pena por el importe del daño y no por el del perjuicio resultante. Todo ello repercutiría en favor de su aplicabilidad a las conductas informáticas.

Lo cierto es que se hace necesaria una reforma de los delitos de daños e incendios en relación no ya sólo a la informática sino a todas las tecnologías de la información y su incidencia en determinados bienes jurídicos dignos de tutela.

Por último y para cerrar el sistema que se propone, el principio de intervención mínima se salvaguarda mediante una política criminal tendente a incriminar sólo las conductas intencionales, excluyendo las culposas y, como es lógico, las debidas a errores técnicos de empleados o fallos de funcionamiento del sistema. Tampoco olvidemos nunca que el Derecho Penal constituye la última ratio, por lo que antes de acudir a él deben agotarse otros recursos, de ahí la conveniencia de coordinar las diferentes vías de protección extrapenal del software: la Propiedad Intelectual e Industrial, en su caso.

EPILOGO

Podemos concluir volviendo a la idea inicial de este trabajo: en los albores del siglo XXI una de las plagas que nos acechan en los países desarrollados son las consecuencias deshumanizantes o indeseables de las nuevas tecnologías. Es preciso adecuar nuestro ordenamiento –en este caso penal– a la situaciones planteadas por la Informática para mitigar esos efectos negativos. Además esa adaptación constituye un proceso contínuo en que por principio el Derecho irá a la zaga de la realidad. Pero por lo menos que el desfase entre aquél y ésta sea el menor posible.

BIBLIOGRAFIA

CAMACHO LOSA, LUIS. «EL Delito informático», Gráficas Cóndor, SA, Madrid, 1987.

CORCOY, MIRENTXU, «Protección penal del sabotaje informático. Especial consideración de los delitos de daños». *La Ley,* 1990, tomo I, págs. 1000 y ss.

CORCOY, MIRENTXU y JOSHI, UJALA, «Delitos contra el patrimonio cometidos por medios informáticos» Revista Jurídica de Cataluña núm. 3.º, 1988. Págs. 133-154.

GONZÁLEZ RUS, JUAN JOSÉ, «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos.» Poder judicial, núm. Especial IX, págs. 39-51.

ROMEO CASABONA, CARLOS MARÍA, «Los delitos de daños en el ámbito informático» Revista de Política Criminal», núm. 43, Madrid, 1991, págs. 91-118.

RUIZ VADILLO, ENRIQUE, «Tratamiento de la delincuencia informática como una de las expresiones de criminalidad económica». Poder Judicial, núm. Especial XI, págs. 53-79.