«Apuntes sobre la perspectiva criminológica de la delincuencia informática patrimonial»

M.ª CARMEN ALASTUEY DOBÓN

Area de Derecho Penal. Facultad de Derecho de la Universidad de Zaragoza

(ESPAÑA)

1. NOCION

Intentar determinar qué se entiende por «criminalidad informática» o más concretamente por «delito informático» no es tarea fácil, sobre todo si se tiene en cuenta que ambas expresiones no han sido aceptadas por la doctrina acríticamente. El término «delito informático» resulta especialmente problemático y ello a pesar de que es utilizado por la mayoría de los autores españoles dada su plasticidad [1]. Se dice, en primer lugar, que no puede hablarse de «delito» para aludir a un comportamiento no tipificado como tal en el C.P.[2] CAMACHO LOSA advierte la falta de tecnicismo del término pero, a pesar de ello, lo usa deliberadamente [3]. Sin embargo, a mi juicio, la principal objeción a dicho término la constituye el hecho de que, como dice ROMEO, no hay un «delito informático» sino una pluralidad de ellos con una única nota común: su vinculación con el ordenador [4]. Por todo esto, quizá resulte más adecuado hablar de «delincuencia o criminalidad informática» como ca-

(1) ROMEO CASABONA, C. «Poder informático y seguridad jurídica». Madrid, 1987 p.41
(2) GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». Madrid, 1991 p.51
(3) CAMACHO LOSA, L. «El delito informático». Madrid, 1987, p. 26
(4) ROMEO CASABONA, C. «Poder informático». cit. p.41

tegoría exclusivamente criminológica [5] en espera de una reforma penal que aclare la situación.

Pero, como apuntaba al principio, la definición del fenómeno no es tampoco unánime. Mencionaré sólo algunas de las definiciones citadas por los autores. TIEDEMANN considera que con la expresión «criminalidad mediante computadoras», se alude a «todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamenteo de datos» [6]. ROMEO se refiere a la definición propuesta por el Departamento de Justicia Norteamericano, según la cual «Delito informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución» [7]. RUIZ VADILLO recoge la definición que adopta el mercado de la OCDE: «Abuso informático es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos» [8], [9].

Por otra parte, surgen nuevos problemas al intentar esclarecer a qué forma de criminalidad se hace referencia cuando se habla de «delincuencia informática». La doctrina, casi unánimemente, la considera inscribible en la criminalidad de «cuello blanco» [10]. Otros la incluyen en la delincuencia económica. RUIZ VADILLO, por ejemplo, cita la Recomendación número R (81) 12 del Consejo de Europa en la que la criminalidad informática es considerada como una forma de la delincuencia económica [11]. El mismo RUIZ VADILLO cree que «toda la fenomenología de la delincuencia económica es aplicable mutatis mutandis a la materia informática» [12]. TIEDEMANN inscribe la «criminalidad mediante computación» entre las formas de criminalidad económica «neutrales», es decir, entre las que surgen en cualquier sistema económico con independencia de la naturaleza del mismo. Por tanto, también TIEDEMANN incluye la «criminalidad por computadoras» entre la criminalidad económica, aludiendo a la parte de aquélla que perjudica los intereses patrimoniales y no a la que perjudica la intimidad [13].

Llegados a este punto, creo que no resulta reiterativo recordar la definición que de delincuencia de «cuello blanco», diera en su día SUTHERLAND:

---

[5] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p.62

[6] TIEDEMANN, K. «Poder económico y delito». Barcelona, 1985. p.122

[7] ROMEO CASABONA, C. «Poder informático». cit. p.42

[8] RUIZ VADILLO, E. «Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica». Poder Judicial. Número especial IX, 1988. pp. 58 y 59

[9] Otros intentos de definición pueden encontrarse en GUTIERREZ FRANCES, M.L. «Fraude informático y estafa». cit. pp. 53 a 58 y en CAMACHO LOSA, L. «El delito informático». cit. pp. 25 y ss.

[10] En este sentido, GUTIERREZ FRANCES, M.L. «Fraude informático y estafa» cit. p.73

[11] RUIZ VADILLO, E. «Tratamiento de la delincuencia informática...» cit. p. 56

[12] RUIZ VADILLO, E. «Tratamiento de la delincuencia informática...» cit. p. 63.

[13] TIEDEMANN, K. «La criminalidad económica como objeto de investigación» Cuadernos de Política Criminal. Número 19, 1983. p.173

«violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional"[14]. Si, además, tenemos en cuenta la definición que se adopta de delincuencia económica desde el punto de vista criminológico, entendiendo por ella la «relativa a las infracciones lesivas del orden económico cometidas por personas de alto nivel socio-económico en el desarrollo de su actividad profesional» [15], deberemos afirmar, que los autores que inscriben la criminalidad informática entre la delincuencia económica, están de acuerdo en inscribirla también entre la delincuencia de «cuello blanco»; y ello aunque consideremos con BAJO que la delincuencia económica es, en puridad, una especie de la de «cuello blanco» y que por eso no debe identificarse aquélla con ésta sin establecer el matiz correspondiente [16]. Pues bien, si analizamos ambas definiciones, encontramos en ellas un elemento común que nos interesa aquí especialmente: el hecho de que el autor de la infracción posea un «alto nivel socio-económico», elemento del que no puede prescindirse en estos conceptos criminológicos porque, como indica BAJO, este elemento evidencia que los efectos de la infracción son más lesivos, por su cuantía, por el número de personas afectadas y porque éstas suelen pertenecer a clases modestas [17]. Ambas definiciones hacen referencia, en consecuencia, a un determinado tipo de autor. Por ello, desde este punto de vista, creo que la delincuencia informática no es subsumible en ninguno de los dos tipos de delincuencia citados, sino que debe constituir una categoría criminológica aparte [18], puesto que en las investigaciones empíricas llevadas a cabo en Estados Unidos, principalmente, se constata que el autor sólo en ocasiones pertenece a las altas capas de la sociedad. Y esto último es reconocido por la doctrina española. Así, ROMEO pone de relieve que los autores suelen ser primarios u ocasionales y que generalmente se trata de empleados de las empresas afectadas [19]. GUTIERREZ se refiere a la caracterización casi mítica que se ha venido efectuando del delincuente informático como adolescente de posición social media (con lo que, por cierto, tampoco entraría en la categoría de delincuente «cuello blanco») y cree que se trata, más bien, de empleados de empresas con acceso a su sistema informático, o incluso chavales jugando con el ordenador o amas de casa [20]. RUIZ VADILLO se muestra reticente a identificar a este tipo de autor con el delincuente propio de la criminalidad de los negocios y caracterizado por las notas que encontró Mer-

---

[14] Véase por todos GARCIA-PABLOS DE MOLINA, A. «Derecho Penal y criminalidad financiera» En su libro «Estudios Penales». Madrid, 1984. p. 288

[15] Definición que «no es más que la adaptación a la delincuencia específicamente económica de la definición que Sutherland en 1939 refirió a la delincuencia de «cuello blanco». BAJO FERNANDEZ, M. «Manual de Derecho Penal. Parte Especial». Madrid, 1987. p. 399

[16] BAJO FERNÁNDEZ, M. «Derecho Penal Económico». Madrid, 1978. p. 49

[17] BAJO FERNÁNDEZ, M. «Derecho Penal Económico». cit. p. 49

[18] En el mismo sentido, RUIZ VADILLO, E. «Tratamiento de la delincuencia informática...» cit. p. 64, siguiendo a TIEDEMANN.

[19] ROMEO CASABONA, C. «Poder informático...». cit. p. 36

[20] GUTIÉRREZ FRANCÉS, M.L. «Fraude informático y estafa». cit. pp. 74 y 79

gen en él, notas con las que elaboró su famoso psicograma [21],[22]. CAMACHO LOSA también cree que los autores de estas infracciones son empleados de confianza de las empresas afectadas, en la mayoría de los casos, que tienen acceso al sistema informático y conocen sus debilidades [23]. Por último, también TIEDEMANN sostiene que los autores suelen ser principiantes o casuales y no poseen una inteligencia superior a la media [24]. No creo que los empleados de las empresas afectadas puedan considerarse personas pertenecientes a las altas capas sociales, en el sentido en que es utilizado el término en el concepto de delincuencia de «cuello blanco». Creo, además, que este concepto debería ser revisado. No todo acto lesivo del orden económico es subsumible en la categoría de delincuencia de «cuello blanco», tendencia muy generalizada hoy en día. Debe atenderse, en cada caso concreto, al tipo de autor [25].

A modo de conclusión: Se ha comprobado que, en la mayoría de las ocasiones, el «delincuente informático» no posee un alto nivel socio-económico y como esta característica es esencial en el concepto de delincuencia de «cuello blanco», creo que la delincuencia informática no puede identificarse, desde un punto de vista criminológico con la reiteradamente citada delincuencia de «cuello blanco».

2. CIFRA NEGRA Y SUS CAUSAS

Es innegable que existe criminalidad informática en España, puesto que las nuevas tecnologías se han implantado también en nuestro país y cuando se generaliza el uso de nuevas tecnologías, aparecen inevitablemente nuevas formas de criminalidad. Sin embargo, resulta imposible calcular la incidencia de dicha criminalidad dada la inexistencia de investigaciones empíricas al respecto, y en España, sólo unos pocos casos han salido a la luz [26]. CAMACHO LOSA se refiere al «muro de silencio que rodea todo lo relacionado con el delito informático» y menciona como «honrosa excepción» al Banco Popular Español que «acostumbra a incluir en sus memorias algunos de estos casos,

---

[21] RUIZ VADILLO. «Tratamiento de la delincuencia informática...» cit.p.63

[22] Mergen intentó determinar las características de la personalidad del delincuente de «cuello blanco» y encontró en ellas las siguientes notas: Materialismo, egocentrismo y narcisismo, dinamismo y audacia, inteligencia, peligrosidad, hipocresía, neurosis y conciencia de culpabilidad. Esta descripción fue muy criticada, pues Mergen no probó como debiera la realidad de sus análisis. Más extensamente en BAJO FERNÁNDEZ, M. «Derecho Penal Económico» cit. pp. 53 y ss.

[23] CAMACHO LOSA, L. «El delito informático». cit. p. 84

[24] TIEDEMANN, K. «Poder económico y delito». cit. p. 126

[25] No debe olvidarse el momento histórico en que surgió el concepto de «delincuente de cuello blanco» ni tampoco los prejuicios neopositivistas de que dicho concepto adolece. Al igual que en la ya superada criminología positivista, se consagra un tipo de autor que, aunque nuevo merece críticas similares. Ver al respecto, GARCIA-PABLOS DE MOLINA, A. «Derecho Penal y criminalidad financiera...» En Estudios Penales. cit. pp. 228 y ss.

[26] ROMEO CASABONA, C. «Poder informático». cit. p. 37

comentando las circunstancias que rodearon el hecho y las consecuencias del mismo» [27]. Pero las investigaciones que se han llevado a cabo en Estados Unidos ponen de relieve que la «zona oscura» más elevada se da en los «delitos perpetrados en conexión con los medios informáticos» [28]. GUTIERREZ, aludiendo a la elevada cifra negra en esta criminalidad, señala que, incluso en los países en que se han detectado un mayor número de casos, éstos sólo representan «la punta del iceberg» [29]. TIEDEMANN pone de manifiesto la imposibilidad de realizar un cálculo siquiera aproximado de la cifra negra en este ámbito y, refiriéndose al caso alemán, señala que, en la mayoría de los procesos penales, el descubrimiento de los hechos se produjo por pura casualidad [30].

Se apuntan varias CAUSAS DE ESTA ELEVADA CIFRA NEGRA EN EL AMBITO DE LA CRIMINALIDAD INFORMATICA.

Por un lado, no existen todavía medios adecuados de detección y control de los hechos. Un sistema complejo de control no resultaría beneficioso a las empresas que precisamente buscaron rentabilidad económica y ahorro de tiempo con la instalación de equipos informáticos [31].

Por otra parte, la víctima desconoce el hecho la mayoría de las veces o, aún conociéndolo y sospechando fundadamente quién lo cometió, tiene dificultades para probar ambas cosas (tanto la perpetración del hecho como su autor). Ciertamente, descubrir el hecho no resulta fácil; las propias características del mismo lo impiden: los medios complejos de comisión del hecho que son conocidos exclusivamente por especialistas en sistemas informáticos, la facilidad del autor de borrar toda huella que pueda inculparle, la separación temporal entre lugar de comisión del hecho y de producción de los efectos, etc. Con todo esto, lo cierto es que estos «delitos» suelen descubrirse por casualidad [32]. A las dificultades de descubrimiento se suman las de prueba en el proceso de estos hechos por las mismas causas señaladas más arriba [33].

En otras muchas ocasiones, la víctima no denuncia los hechos, pues teme que, reconocer que ha sido objeto de uno o varios de estos comporta-

---

[27] CAMACHO LOSA, L. «El delito informático». cit. p. 69

[28] ROMEO CASABONA, C. «Poder informático». cit. p. 36. Advierte ROMEO que cuantificar la zona oscura resulta difícil puesto que los estudios criminológicos al respecto no son suficientemente rigurosos.

[29] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p. 72

[30] TIEDEMANN, K. «Poder económico y delito». cit. p. 123

[31] ROMEO CASABONA, C. «Poder informático». cit. p. 38. También CAMACHO LOSA, L. «El delito informático» cit. p. 70, hace referencia a la casi total ausencia de medidas de seguridad en las instalaciones.

[32] Véase, por todos, CAMACHO LOSA, L. «El delito informático», cit. p. 70, apunta que, probablemente los casos conocidos hubieran quedado en el anonimato de no ser por la casualidad.

[33] GUTIÉRREZ FRANCÉS, M. L «Fraude informático y estafa» cit. pp. 80 y 81.

mientos, pueda incidir negativamente en el buen nombre de la empresa, con la natural desconfianza hacia la misma por parte de los clientes de la entidad que surgiría al comprobar que carecía de las medidas de seguridad adecuadas. Además, a las empresas afectadas les resulta más rentable una solución privada del problema, pues, como dice TIEDEMANN, consideran que si se impusiera una pena privativa de libertad al autor del hecho, dejaría de trabajar y de percibir una remuneración, con lo que disminuiría considerablemente la posibilidad de aquél de reparar el daño causado [34]. Por otro lado, la víctima (en general y no sólo la de delincuencia informática), desconfía de que los tribunales puedan solucionar su problema [35].

CAMACHO LOSA añade entre las causas que influyen en el hecho de que los autores de un delito informático no sean denunciados, la falta de una legislación adecuada al respecto [36].

3. LA VICTIMA

Como puede deducirse de las páginas anteriores y como demuestra la experiencia extranjera y los pocos casos que se han dado a conocer en España, las víctimas del ilícito informático son, casi sin excepción, personas jurídicas. Parece ser que, por regla general, se trata de bancos o compañías de seguros o empresas del sector pero, como advierte ROMEO, también las empresas públicas son víctimas de estos ilícitos y pone como ejemplo de estos últimos casos las diversas actividades de los servicios postales o de la Seguridad Social [37].

También mediante la observación de los casos conocidos, GUTIERREZ llega a la conclusión de que suele tratarse de «personas jurídicas con un potencial económico muy elevado, y que, por lo general, no gozan de muy buena prensa entre el ciudadano medio». Además, y enlazando con el apartado anterior, las víctimas suelen actuar como «colaboradoras» del hecho: rara vez denuncian las conductas ilícitas, en pocas empresas se protegen los sistemas informáticos con medidas de seguridad y controles adecuados, las empresas cometen a veces errores que propician la comisión del hecho al autor potencial.... [38]

4. LOS HECHOS

Las características de los hechos, aunque fácilmente deducibles de lo ya examinado hasta ahora, pueden resumirse de este modo:

---

[34] TIEDEMANN, K. «Poder económico y delito». cit. 123. Ver también ROMEO CASABONA, C. «Poder informático». cit. p. 39 y RUIZ VADILLO, E. «Tratamiento de la delincuencia informática... cit. p. 57

[35] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p.72

[36] CAMACHO LOSA, L. «El delito informático». cit. p. 70

[37] ROMEO CASABONA. C. «Poder informático». cit. p. 39

[38] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa» cit. p. 76

a) Estos hechos procuran a sus autores unas elevadas ganancias. El perjuicio económico que producen es muy superior al de cualquier otro tipo de conducta ilícita, también al causado por la delincuencia económica. Se da, además, el anonimato del perjuicio producido [39].

b) Por regla general, estas conductas no se llevan a cabo con un único acto sino mediante una serie continuada de ellos. Es decir, esta forma de delincuencia tiene un EFECTO CONTINUADO. Si en la primera intromisión en el sistema informático se logra tener éxito, el autor suele continuar con la comisión de actos ilícitos [40].

c) Entre el hecho ilícito y los efectos del mismo existe una separación temporal [41].

d) Una vez cometido el ilícito, el autor consigue borrar todas las huellas, sin dejar rastro perceptible, lo que hace que disminuya considerablemente el riesgo de ser descubierto [42].

e) Los autores del «delito» no suelen ser personas con una inteligencia superior a la media que poseen conocimientos cualificados en el campo de la informática y que por ello llevan a cabo manipulaciones sofisticadas en los sistemas informáticos, sino más bien personas con un coeficiente intelectual medio, que tienen la «oportunidad» de realizar el hecho y la aprovechan [43]. En este sentido, creo que el móvil del autor es, en la mayor parte de los casos, «sencillamente», el ánimo de lucro, aunque pueda haber otros móviles complementarios [44].

5. POSIBLES SOLUCIONES

Para luchar contra la delincuencia informática, las medidas preventivas juegan un papel primordial. Las empresas se muestran reacias a proteger su

---

[39] ROMEO CASABONA, C. «Poder informático». cit. p.35, GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. pp. 78 y 79. CAMACHO LOSA, L. «El delito informático». cit. pp. 69 y ss, GONZÁLEZ RUS, J. J. «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos» Revista de la Facultad de Derecho de la Universidad Complutense de Madrid. Número 12. Monográfico sobre informática y derecho, 1986. TIEDEMANN, K. «Poder económico y delito». cit, pp. 123 y ss y otros.

[40] Véase TIEDEMANN. K. «Poder económico y delito» cit. p. 123 y en el mismo sentido GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p. 79

[41] Véase nota anterior.

[42] GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa» cit. p. 79 y ROMEO CASABONA, C. «Poder informático» cit. p. 35

[43] En este sentido CAMACHO LOSA. L «El delito informático» cit. p. 83 asegura que el perfil de estas personas en general no es el de un delincuente, sino que «se trata de personas que podríamos encuadrar en lo que coloquialmente denominamos gente del montón que por azar, por diversión, o por investigación técnica han descubierto ciertas debilidades en el sistema que les pone en situación de poder aprovecharse de dicha circunstancia, y coyunturalmente se encuentran en una situación en la que sin ser desesperada no les vendría mal un puñado de dinero extra».

[44] Ver GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa» cit. p. 75 y 76. También GONZÁLEZ RUS, J.J. «Aproximación al tratamiento penal» cit. p. 111.

sistema informático de manipulaciones ilícitas mediante la adopción de rigurosas medidas de seguridad y controles pues supondría una pérdida considerable de tiempo y dinero que, creen los directivos de algunas entidades, superaría quizá el perjuicio económico causado por un «delito» informático esporádico y aislado. Es verdad, como CAMACHO LOSA deja patente [45], que la adopción de sistemas de seguridad de esta envergadura, supone un esfuerzo de trabajo, económico, el nacimiento de nuevas responsabilidades, la necesidad constante de renovación de dicho sistema. Pero, como el mismo autor señala, estos controles permitirían detectar la situación anormal y frecuentemente minimizar sus consecuencias; y en todo caso, posibilitarían descubrir al autor y probar su culpa ante los tribunales [46].

Pero sin acudir a estas sofisticadas medidas, existen otras más fáciles de poner en práctica por parte de las empresas y con ellas es posible obtener resultados satisfactorios. Entre estas medidas se cuentan: la separación física del departamento de informática del resto de las instalaciones de la empresa; la separación de funciones, de modo que no cualquier empleado pueda acceder a los ordenadores; el cambio frecuente de los códigos de acceso; la identificación de los empleados autorizados para el uso del ordenador cada vez que vayan a manejarlos; la posibilidad de que las terminales se desconecten automáticamente tras cierto tiempo de inactividad; la realización de auditorías internas y externas con expertos informáticos e incluso el concierto de seguros para cubrir los riesgos de los perjuicios derivados de un posible ilícito informático [47].

La delincuencia informática patrimonial puede prevenirse más fácilmente que la delincuencia clásica contra el patrimonio. Pero cuando las medidas preventivas que se adopten no resulten suficientes para evitar la comisión del hecho (o bien no se ha adoptado ninguna) y el ilícito se haya cometido efectivamente, deberán determinarse las sanciones que se aplicarán a su autor o autores. La pregunta clave a este respecto es si es o no conveniente la introducción en el C. P. de nuevos preceptos que recojan estos comportamientos y establezcan sanciones para los mismos o bien si, por contra, es posible castigar las mencionadas conductas mediante tipos penales ya existentes [48].

Para empezar, consideraré la conducta aisladamente, con independencia de su autor. En mi opinión, atendiendo a las clasificaciones más o menos

---

[45] CAMACHO LOSA, L. «El delito informático». cit. pp.143 y ss.

[46] CAMACHO LOSA, L. «El delito informático». cit. p. 73

[47] ROMEO CASABONA, C. «Poder informático» cit. p. 40 y GUTIÉRREZ FRANCÉS, M. L. «Fraude informático y estafa». cit. p.83

[48] RIVERO CORNELIO, A.M. «Informática y Derecho. La Informática Jurídica en España». Revista de la Facultad de Derecho de la Universidad Complutense de Madrid. Número 12, Monográfico sobre Informática y Derecho, 1986. p.201. Se plantea «si la utilización masiva de los ordenadores y la telemática puede cambiar la naturaleza y el alcance de la conducta delictiva (...) si puede llegar a configurar nuevos tipos de delito y (...) si es necesario dotar a la sociedad de unos medios jurídicos específicos para su protección y defensa».

coincidentes que la doctrina española viene elaborando sobre modalidades de comportamientos delictivos inscribibles en la delincuencia informática [49], estos comportamientos pueden subsumirse en preceptos actuales de nuestro C. P. (falsedades, estafas, hurto, robo, daños...) sin necesidad de crear unos nuevos. Es obvio que la delincuencia informática patrimonial presenta caracteres específicos que la diferencian de la criminalidad patrimonial «clásica»; sin embargo, creo que estas especificidades tienen, predominantemente, un interés criminológico o, desde un punto de vista procesal, afectan a las dificultades de descubrimiento y prueba de los hechos. No me parece que estas características diferenciadoras puedan servir como argumento para la introducción en el C. P. de preceptos en los que se recojan los citados comportamientos. Como apuntaba al tratar de definir la delincuencia informática patrimonial, creo con ROMEO que estamos ante una pluralidad de delitos que tienen, como única nota común, su vinculación con los ordenadores [50]. La nota diferenciadora por excelencia la constituye la concurrencia de un ordenador en alguna o todas las fases de ejecución del delito. No cabe duda de que se trata de un elemento diferenciador muy considerable, pero a pesar de ello no afecta, a mi juicio al contenido básico a la «sustancia del delito» [51], [52]. En todo caso, podría servir de base para la creación de tipos agravados respecto de los básicos ya existentes.

El delincuente informático, por otra parte, no se identifica con la imagen que la opinión pública se ha forjado del delincuente «clásico» contra el patrimonio. Desde este punto de vista se cuestiona la aplicación de sanciones penales a los delincuentes informáticos aludiendo a su «incapacidad de motivación». Sin embargo, respetando siempre el principio de intervención mínima del Derecho Penal, la sanción penal deberá aplicarse cuando sea necesario, también al delincuente informático. Atendiendo en primer lugar al principio de proporcionalidad de las penas, no olvidemos los cuantiosos perjuicios patrimoniales que causan estas conductas, perjuicios que las hacen merecedoras, en mi opinión, de un reproche mayor que el que conlleva la sanción administrativa. Se argumenta también, en contra de la aplicación de sanciones penales a este tipo de delincuentes, que no tienen conciencia de actuar de forma ilícita. No creo que esta sea una característica específica del delincuente informático sino que, por contra, se da en otras muchas manifestaciones de delincuencia. Por otra parte, el hecho de que el control penal sea poco eficaz en este tipo de delincuencia, dada la elevada cifra negra que se

[49] Ver clasificación de GONZÁLEZ RUS, J. J. «Aproximación al tratamiento penal...» cit. pp. 116 y ss.

[50] Ver nota 1.

[51] RUIZ VADILLO. E «Tratamiento de la delincuencia informática» cit. p. 72

[52] Supera el objetivo de esta ponencia el análisis minucioso de cada uno de los comportamientos delictivos llevados a cabo mediante o sobre sistemas informáticos para determinar así en qué precepto del C.P. pueden subsumirse. En este sentido remito a ROMEO CASABONA, C. «Poder informático» cit. desde la p. 47

intuye, no es argumento suficiente para propugnar la no aplicación de sanciones penales, sino para meditar sobre posibles mejoras de los mecanismos de control. Por último, y por lo que respecta a la aplicación de la pena privativa de libertad a estos delincuentes, se ha dicho que ésta no puede cumplir el fin resocializador que le otorga la Constitución en el art. 25.2º , puesto que estos delincuentes no necesitan resocialización [53]. No estoy de acuerdo con esta apreciación. Entiendo por reinserción social la «capacitación para vivir en sociedad sin infringir notablemente las leyes penales» [54], y en este sentido está claro que estos delincuentes necesitan de reinserción social. Hoy en día, ciertamente, el fin resocializador de la pena está sumido en una profunda crisis: la pena no resocializa, «pero no resocializa a nadie. ¿Por qué ha de merecer un régimen discriminatorio este autor?» [55].

Para concluir y a modo de resumen: puede deducirse de las características de los hechos, que el establecimiento de medidas preventivas resulta muy eficaz para evitar la comisión de ilícitos mediante procedimientos informáticos. Una vez cometido el hecho, descubierto su autor y salvadas las dificultades procesales (esto es posible en pocas ocasiones, pero no por ello debe dejar de plantearse el supuesto), deberán aplicarse al autor las sanciones previstas en los preceptos penales en los que sea subsumible su conducta, siempre que ésta, naturalmente constituya delito.

BIBLIOGRAFIA

BAJO FERNÁNDEZ, M. Manual de Derecho Penal. Parte Especial. II. Delitos patrimoniales y económicos. Ed. Ceura. Madrid, 1987. – Derecho Penal económico. Ed. Civitas. Madrid, 1978.

BERISTAIN IPIÑA, A. «Eficacia de las sanciones penales frente a la delincuencia económica». Indice Penale. Ed. Cedam-Padova, 1982.

CAMACHO LOSA, L. El delito informático. Ed. Ministerio de Cultura. Madrid, 1987.

GARCÍA-PABLOS DE MOLINA, A. Estudios Penales. Ed. Bosch. Madrid, 1984.

GONZÁLEZ RUS, J. J. «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos». Revista de la Facultad de Derecho de la Universidad Complutense de Madrid. Número 12. Monográfico sobre Informática y Derecho. 1986.

[53] Utilizo el término «resocialización» como sinónimo de «reinserción social». Sobre los problemas que plantea el término «resocialización» véase GARCÍA-PABLOS DE MOLINA, A «La supuesta función resocializadora del Derecho Penal» En Estudios Penales cit. pp 22 a 27.

[54] BERISTAIN IPIÑA, A. «Eficacia de las sanciones penales frente a la delincuencia económica». L. Indice Penale 1982

[55] GARCÍA-PABLOS DE MOLINA, A. «Derecho Penal y criminalidad financiera». En Estudios Penales cit. p. 244. Ver también la nota 139 en la misma página. La palabra «autor» de la frase que transcribo, aunque se refiere al autor de delitos económicos y no propiamente al delincuente informático, creo que resulta trasladable a este contexto.

GUTIÉRREZ FRANCÉS, M. L. Fraude infomático y estafa. Ed. Centro de publicaciones del Ministerio de Justicia. Madrid, 1991.

ROMEO CASABONA, C. Poder informático y seguridad jurídica. Ed. Fundesco. Madrid, 1987.

RIVERO CORNELIO, A. M. «Informática y Derecho: La Informática Jurídica en España». Revista de la Facultad de Derecho de la Universidad Complutense de Madrid. Número 12. Monográfico sobre Informática y Derecho. 1986.

RUIZ VADILLO, E. «Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica». Poder judicial. Número especial IX. 1988.

TIEDEMANN, K. Poder económico y delito. Ed. Ariel. Barcelona, 1985. «La criminalidad económica como objeto de investigación». Cuadernos de Política Criminal. Número 19. 1983.