LA PENALIDAD DEL DELITO DE PROGRAMA DE ORDENADOR FRAUDULENTO EN EL CÓDIGO PENAL ESPAÑOL. RÉGIMEN VIGENTE Y POSIBILIDADES DE REFORMA

The penalty of the crime of fraudulent computer program in the spanish penal code. current situation and possibilities for reform

Roberto Cruz Palmera
Doctor en Derecho. Profesor de Derecho Penal
Universidad Autónoma del Caribe (Barranquilla, Colombia)
rcruz.3@alumni.unav.es

http://dx.doi.org/10.18543/ed-68(2)-2020pp75-95

Recibido: 04.12.2020
Aceptado: 21.12.2020

Resumen

En esta contribución presentamos un nuevo estudio del delito de «programa de ordenador fraudulento», art. 248.2 b) del Código Penal español. Se trata de una revisión de los aspectos más problemáticos: el adelantamiento de las barreras de protección y la penalidad. Exponemos en estas páginas una propuesta de reforma que intenta sanear la desproporcionalidad de la pena y los problemas derivados de la excesiva anticipación punitiva.

Palabras clave

Fraude. Proporcionalidad. Preparación.

Abstract

In these pages we present a new study of the crime of «fraudulent computer program», art. 248.2 b) of the Spanish Penal Code. It is a review of the most problematic aspects, the advancement of protection barriers and the penalty. We propose a proposal to reform the penalty that tries to be more proportional to the content of the injustice and to the problems derived from punitive anticipation.

Keywords

Fraud. Proportionality. Preparation.

Sumario: I. Planteamiento. II. Aspectos problemáticos. III. Valoración de las conductas incriminadas. IV. Valoración crítica. V. Reflexión final y propuesta de *lege ferenda*. VI. Conclusiones. Bibliografía

I. PLANTEAMIENTO

La defensa jurídica del patrimonio económico responde a una exigencia constitucional[1]. La Constitución española y el Código Penal[2] nos muestran dispositivos destinados a la protección de ese bien jurídico. Este instrumento busca resguardar el patrimonio económico al verse amenazado ante herramientas tecnológicas potencialmente lesivas para el patrimonio de los ciudadanos. Los nuevos tiempos obligan a adaptar la legislación ante novedosas formas delictivas que dejan a los ciudadanos en un elevado grado de indefensión. Este motivo, hasta cierto punto, parecería justificar el drástico adelantamiento de las barreras de punibilidad[3] y la desproporcionada sanción que

[1] * Para las citas jurisprudenciales opté por la base de datos vLex España.

El precepto contenido en el art. 2482. b) del Código Penal se le conoce mayoritariamente en la doctrina científica como «Acto preparatorio relativo a programas informático específicamente destinados a la comisión de estafas». En realidad lo se castigan cuatro conductas: fabricación, introducción, posesión y facilitación de un programa fraudulento para causar una lesión patrimonial. Optamos por denominarlo «programa de ordenador fraudulento» no para descontextualizarlo, pues no negamos que se ubica dentro de las denominadas estafas, sino optamos por esa expresión para tratar de explicar mejor la naturaleza instrumental y preparatoria de ese delito. Al respecto, véase (Dopico Gómez-Aller 2018, 231-232).

Véase el artículo 33 CE: «1. Se reconoce el Derecho a la propiedad privada y a la herencia». En efecto, la tipificación de un delito contra la propiedad privada tiene como fundamento la protección de un derecho reconocido por la Constitución que se esconde, por decirlo de alga manera, también en el tipo; o, mejor dicho, mediante este instrumento, la propiedad se protege a través de los preceptos que regulan los delitos contra el patrimonio y orden socio económico.

[2] Artículo 248.2 b): «También se consideran reos de estafa: Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo».

[3] (Muñoz Conde 2019, 393-394): «[…] la equiparación a efectos de pena de estas conductas a la estafa propiamente dicha tipificada en el apartado 1 es discutible, ya que, en realidad, se trata de actos preparatorios o todo lo más de tentativa de estafa. La razón de esta equiparación punitiva se debe a la importancia que tienen actualmente los programas informáticos en el tráfico económico en general y a que de este modo se le otorga una protección especial reforzada al sistema informático como bien jurídico colectivo. Ello daría lugar a entender estas conductas como delitos de peligro abstracto y a considerar que cabe el concurso entre ellas y el delito posterior de estafa que se cometa».

caracteriza al «delito de programa de ordenador fraudulento». El precepto contenido en el art. 248.2 b) reza como sigue: «También se consideran reos de estafa: Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo». Pasemos a revisarlo con más detenimiento.

El legislador español al incluir el «delito de programa de ordenador fraudulento», pretende evitar una peculiar modalidad delictiva que atenta contra el patrimonio de las personas. Es evidente que el bien jurídico tutelado en el precepto contenido en el art. 248.2 b) es el patrimonio económico; sin embargo, es evidente que ante un excesivo adelantamiento de las barreras de protección penal ese bien jurídico se represente demasiado alejado de las acciones incriminadas en la norma, lo cual hace imposible una lesión o afectación. Otro punto de vista, menos tradicional, sostiene que los programas de ordenador fraudulento perturban, por decirlo de algún modo, la tranquilidad en las transacciones mercantiles, un derecho merecedor de protección. Bajo esta posición, «la tranquilidad en las transacciones mercantiles» el precepto serviría para garantizar la protección de los métodos de disposición de los bienes jurídicos relacionados en la dinámica mercantil; no solo los valores conexos en compraventa, también, los fondos que reposan en las cuentas bancarias, así como cualquier elemento que represente un valor en las actividades ordinarias relacionado en las transacciones mercantiles[4]. Independientemente de las posiciones que se tengan respecto al bien jurídico, lo cierto es que mediante el «delito de programa de ordenador fraudulento» se intenta garantizar la *normalidad* en todos los movimientos económicos distintos al efectivo, una misión relativamente imposible a la altura de los tiempos[5].

II. ASPECTOS PROBLEMÁTICOS

El precepto contenido en el art. 248.2 b) demuestra una «deficiente técnica legislativa»[6]; protege un bien jurídico que ya se encuentra protegido en

[4] (Tavares 2010, 210-218). Se refiere a los denominados métodos de disponibilidad. En el caso de las defraudaciones o estafas informáticas, el método seria todo el aparato que envuelve el proceso de las transacciones. Si no lo mal interpreto, el método de disponibilidad, siguiendo el planteamiento trazado por el autor, es accesorio respecto a los bienes jurídicos, por lo tanto, sin el bien jurídico el método de disponibilidad desaparecería por completo, no tiene cabida en el mundo por sí mismo, puesto que ha sido creado para hacer factible el uso y disfrute de los derechos que —por decirlo de alguna manera— se esconden tras los bienes jurídicos.

[5] STS 20 noviembre 2001 (RJ 2002\805 Martínez Arrieta), F.J. 1. En ese orden, la jurisprudencia sostiene que se busca prevenir manipulaciones tanto de entrada como de salida de datos que pueden afectar los intereses económicos protegidos.

[6] De igual opinión, (Cruz de Pablo 2006, 46-47).

Estudios de Deusto
© Universidad de Deusto • ISSN 0423-4847 • ISSN-e 2386-9062, Vol. 68/2, julio-diciembre 2020, págs. 75-95
http://dx.doi.org/10.18543/ed-68(2)-2020pp75-95 • http://www.revista-estudios.deusto.es/

el mismo cuerpo normativo[7], piénsese, sin ir más lejos, en la tentativa de estafa informática o en la perfecta realización del delito de fraude informático (delito fin o tipo base).

Al precepto se le define como delito de peligro abstracto[8], como forma de intervención o participación anticipada, además, como un acto de preparación elevado a la categoría de delito de estafa[9]. La mayoría de las valoraciones obedecen a un intento de categorización, pero entendemos que su naturaleza obedece a un «delito instrumental». Al realizar una lectura mesurada encontramos que instituciones como la participación, la tentativa y el desistimiento voluntario, son tanto de difícil determinación. Sancionar la participación o la tentativa de una acción que aún no representa ni peligro si lesión al bien jurídico protegido pondría en tela de juicio, al menos, el principio de lesión.

Además, ante una *desmesurada* anticipación de las barreras de protección, sancionar la tentativa del delito de «programa de ordenador fraudulento» se tornaría poco conveniente ante en un sistema respetuoso del principio del hecho[10]. También, respecto a la participación, podemos decir que se extendería aún más el alcance de la norma a conductas que en poco o en nada contribuyan en la afectación real de un interés jurídico, produciéndose sendas contradicciones con el principio de culpabilidad[11]. Ante el incre-

[7] Creo que sería muy difícil refutar que el bien jurídico protegido, esto es, a mi modo de ver, el patrimonio económico, no cuente con protección en otros preceptos en el mismo código; sin embargo, se discute el objeto de protección, valoración que agotaremos en su oportunidad en esta sección.

[8] (Faraldo Cabana 2009, 112-113).

[9] (Anarte Borrallo y Doval Pais 2012, 242-243); (Faraldo Cabana 2009, 110-111)

[10] El castigo de la tentativa debería analizarse con lente crítica para esta clase de preceptos, aunque técnicamente sea factible (art. 16.1 del CP). Los motivos para rechazar su aplicación obedecen a los graves excesos que se producirían con su aplicación, piénsese que sancionar la tentativa de la preparación desbordaría el merecimiento del reproche desde el punto de visa del Derecho penal. La sanción de la tentativa es posible, pero inviable desde un punto de vista político criminal, puesto que aplicar la tentativa de actos preparatorios autónomos para la comisión de una estafa, no constituye aún una forma de ataque que merezca un reproche penal, dado la inobjetable ausencia de lesión y puesta en peligro para el bien jurídico.

[11] (Roxin 1981, 47-163).

Casi nada impediría que «A» fabrique un programa para defraudar, pero este (fabricador) puede afectar con su conducta a otras personas que no participaron en la fabricación; puesto que «A» (fabricador) puede instalar dicho programa en el ordenador de «B», su compañero de trabajo. De manera que al nuevo «poseedor» se le podrías sancionar por el delito de tenencia de programas informáticos para la comisión de estafa. Así planteado el problema, la siguiente idea derivada del principio de la culpabilidad quedaría en tela de juicio: nadie tiene por qué asumir la responsabilidad de la conducta realizada por otro.

mento del ámbito de prohibición es todavía más criticable el bien jurídico elegido, dudamos que merezca la utilización de esta figura, pues protege un interés de consideración jurídica importante, pero no lo suficientemente relevante como para admitir la sanción de actos preparatorios.

Un aspecto relevante en el delito de «programa de ordenador fraudulento» son los objetos del delito (nos referimos a los programas informáticos). Sobre el particular, conviene analizar si un programa de ordenador que sirve para conseguir una trasferencia bancaria no autorizada y a su vez pueda ser utilizado para actividades neutrales –como la recopilación sistemática y envió de datos– debe ser objeto de sanción. Otro asunto que también resulta controvertido, como dijimos, es la determinación del bien jurídico protegido. Lo común es afirmar que el objeto de protección sea el patrimonio económico; este se ve amenazado con los programas informáticos debido a la capacidad delictiva, dado que pueden conseguir una transferencia económica. Otra concepción es considerar objeto de protección el sistema informático como bien jurídico colectivo[12], una posición sugerente, pero resulta problemática. El desarrollo vigente de estas opiniones se deben al drástico adelantamiento de las barreras de punición, dado que la tipificación de conductas tan imprecisas obligan a encontrar un bien jurídico susceptible de lesión, dicho de otra manera, la vaguedad de las acciones, sumando una desmesurada anticipación de la tutela penal supone la búsqueda de un bien jurídico que pueda ser lesionado o afectado; por ejemplo, mediante, la «tenencia» de objetos peligrosos. No olvidemos que se incrimina la «fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados a la comisión de estafas»; sin que sea necesario defraudar a otro: todas son acciones de disposición [13].

[12] (Muñoz Conde y García Arán 2015, 349-348). Al respecto, afirma que el bien jurídico protegido es el sistema informático, puesto que el Derecho penal le otorga una protección debido al «protagonismo» de estos sistemas en las relaciones mercantiles, métodos de pago, etc. Por cierto, en cuanto a la discusión del bien jurídico se han levantado otras posturas diferentes, pues algunos autores afirman que el objeto de protección es la propiedad, pero desde una perspectiva más amplia que la comúnmente utilizada por el Código Civil, debe mirarse el concepto de propiedad desde un panorama constitucional. En esta dirección, se sostiene que el término patrimonio no es del todo adecuado, ya que dentro de esa noción se podrían incluir, entre otros conceptos, las deudas. (Aboso y Zapata 2006, 74-77).

[13] Casi todos compartimos que la tentativa, de cualquier delito, debería ser el límite del poder punitivo respecto a la anticipación, pero vemos que con esta clase de tipos penales se busca externarse más de lo racionalmente posible. En muchos casos, podemos corroborar que, aunque el sujeto activo materialice actos posteriores a la ideación del proyecto delictivo —en el mundo fenoménico—, estos no logran ser punibles a pesar de su univocidad delictiva, me refiero a la preparación. Pongo un ejemplo de manual: el sujeto parado delante de una puerta de una casa con una ganzúa en el bolsillo no incurre

Admitir la «tranquilidad de las transacciones bancarias, mercantiles», o la protección del «sistema informático» sería improvisar un bien jurídico que resulta inabarcable, indeterminado[14]… Resultaría muy complejo encontrar criterios específicos para establecer qué clase de conductas crean, en realidad, un riesgo jurídicamente relevante para lesionar o afectar intereses jurídicos como «la tranquilidad». Expresiones como «el derecho a comprar en paz», «la tranquilidad en los movimientos bancarios» o «la estabilidad del sistema informático» carecen de objetividad, estas dependen del grado de susceptibilidad de cada persona, así como de otros factores sociológicos como el conocimiento de experiencias de terceros que han sido afectados mediante instrumentos maliciosos. La tecnología –en nuestro tiempo– avanza de continuo y muchas conductas podrán amenazar tanto el «sistema informático» como «la tranquilidad en las transacciones». Esas nociones desarticulan el concepto de bien jurídico y evidencian la utilización del Derecho penal como herramienta de protección urgente; sin embargo, el bien jurídico debe ser límite del poder punitivo; no un instrumento para justificar la expansión punitiva[15]. Pero en lo que casi todos estamos de acuerdo, es que los ciudadanos no están dispuestos a tolerar ninguna clase de fraude y menos mediante programas o instrumentos maliciosos que ponen en desventaja a los titulares de las cuentas bancarias.

Por todo lo anterior, vemos que el precepto requiere la fijación de criterios limitadores para que el operador judicial pueda interpretarlo y aplicarlo. En ese sentido, es necesario establecer qué es lo que en realidad protege la

todavía en una tentativa de robo. Sin embargo, en «el delito de programa de ordenador fraudulento» podemos ver, incluso, que resulta más conveniente intentar la materialización del delito base («defraudación informática») que caer en la red de la preparación delictiva que caracteriza a la norma (art. 248.2 b]). Irónicamente, la incriminación de esos actos preparatorios se castiga con una pena más elevada que la prevista para la tentativa del delito base.

[14] Así, (Zaffaroni 2006, 375-376): «La creación de peligros y por ende, de ofensas artificiales, no sólo pretende presumir ofensas inexistentes, sino que inventa y clona bienes jurídicos: (a) se inventan bienes jurídicos cada vez que se menciona la seguridad, la paz general, el bien público, etc., que son el resultado del aseguramiento de todos los bienes jurídicos; (b) se clonan bienes jurídicos creando supuestos bienes jurídicos intermedios (cuya afectación es lesiva sólo por poner en peligro otros bienes jurídicos, como la falsedad documental), o sea que se tipifica un acto preparatorio de otra tipicidad y, para colmo, se habilita el poder punitivo también con la tentativa, con lo cual pretende tipificarse la tentativa de un acto previo a la tentativa (preparatorio). Estas artimañas autoritarias, por un lado ocultan una violación al art. 19 constitucional y, por otra, al dejar en un cono de sombra la determinación de la existencia del peligro como requisito típico, violan el principio que exige el máximo de precisión posible respecto de cualquier límite de prohibición –principio de máxima taxatividad».

[15] (Silva Sánchez 2012, 456-457).

norma[16], valoración que debería realizarse dentro del sistema integral de Derecho penal; no mediante valoraciones meramente sociológicas pese a su importancia. Actualmente se aplican sanciones por poseer, fabricar, o facilitar instrumentos para cometer una defraudación[17]. A nuestro modo de ver, podría plantearse la utilización de otro mecanismo distinto al Derecho penal para regular la posesión, fabricación o facilitación, pues a día de hoy esta norma nos muestra un quebrantamiento de principios básicos como el de culpabilidad, subsidiaridad, principio del hecho y lesividad[18], sin olvidarnos de una desmesurada equiparación de estafa a lo que son meras predisposición delictiva, predisposición a las que se les asigna una penal irracional[19]. Volvamos al bien jurídico. Si admitimos, por un lado, que se protege el patrimonio económico, estaríamos anticipando la intervención a lo que no logra constituirse todavía ni siquiera en una tentativa de estafa[20]. Existe una gran distancia entre la facilitación o fabricación de un programa para estafar y la disminución de un saldo en la cuenta bancaria de otro. No son fáciles de quebrantar los métodos de protección que se exigen a la hora de autorizar movimientos bancarios (por ejemplo: la inclusión de códigos de la cybertarjeta de pago, las claves enviadas al teléfono móvil para confirmar una compra, la ratificación telefónica de algunos movimientos realizados por Internet, la necesidad de dar respuestas a preguntas de seguridad, etc.). Del mismo modo, resulta difícil argumentar que el patrimonio económico se afecte inmediatamente con la aparición aislada de estos programas. Por otro lado, aceptar que el bien jurídico protegido sea el «sistema informático» como medio necesario en las relaciones mercantiles, sería contradictorio, pues el precepto contenido en el art. 248.2 b) está ubicado en los denominados delitos contra el patrimonio económico, por lo cual resultaría provechoso regular la protección por otra vía distinta al Derecho Penal. En todo caso, como hemos mostrado en etas páginas, se trata de blindar a los ciudadanos de cualquier clase de ataque que provenga de manipulaciones mediante programas

[16] (Mir Puig 2015, 175-176).

[17] Véase, entre otras, la STS 9 de mayo de 2007 (RJ 369\2007 Berdugo Gómez de la Torre), F.J. 1-4.

[18] (Romeo Casabona, en Romeo Casabona y Boldova Pasamar coords. 2016 367-368).

[19] (Queralt Jiménez 2010, 519-520). Asegura que la pena establecida por el legislador es desde todo punto de vista ilegítima a razón de su desproporcionalidad. Con toda razón, pues la proporción, a mi juicio, es un ideal de la Justicia en el más amplio de los sentidos.

[20] (Pastor Muñoz 2005, 65-66), sobre este particular, sostiene que esta incriminación: «[…] tendría sentido si se pudiera afirmar que los comportamientos tipificados en aquellos no son perturbaciones sociales, sino descripciones de estados peligrosos. Y ello no es así, pues la pena de estos tipos no es una reacción frente a la peligrosidad subjetiva, sino frente a la manifestación de la peligrosidad subjetiva».

informáticos, esto puede ser factible, siempre que no se infrinjan los principios básicos del Derecho penal como lo es el principio de proporcionalidad[21]. Resulta desacertado aplicar una misma pena tanto para el delito base como para las acciones preparatorias del delito fin[22] («defraudación informática» o «estafa informática»)[23].

Los titulares de las cuentas bancarias deben intensificar las barreras de protección, en esto estaríamos casi todos de acuerdo; por lo que se sugiere cuidar la privacidad de los datos de sus tarjetas bancarias en los movimientos mercantiles, realizando las transacciones y demás movimientos con dispositivos propios, esto es, no de personas desconocidas. Además, ingresando en la plataforma bancaria mediante redes seguras, o sea, evitando la conexión en zonas libres. Conjuntamente, evitar la utilización de la misma clave o contraseña de la cuenta bancaria para dispositivos como tabletas, ordenadores, teléfonos móviles, etc. Sin embargo, casi nadie negaría que los bancos deben proteger tanto las bases de datos de sus clientes como los mecanismos de pago para garantizar dichos movimientos. Las entidades bancarias están en la obligación de velar por la tranquilidad de sus clientes en la dinámica mercantil. De no ser así: ¿qué razón tendría que las personas confiaran en estas entidades parte de su dinero? En similar sentido, los establecimientos comerciales están en el deber de ofrecer tranquilidad y confianza en los medios de pago de sus clientes, por ejemplo, garantizando transparencia en las transacciones mediante el uso de los datáfonos, así como otros medios de desembolso electrónico[24]. De otro modo: ¿qué sentido tendría que estas entidades se lucren

[21] En similar sentido, cfr. STC 22 de julio 2010 (RJ 2755\2007 Delgado Barrrio) F.J. 1-2.

[22] La asignación arbitraria de la pena, como vemos en este supuesto, se fundamenta en una conminación político criminal que refuerza la protección del patrimonio económico; no estante, estas medidas se toman sin tener en cuenta la función preventiva de la pena y la constatación de los objetivos buscados por el legislador.

[23] Así, STS 16 de octubre 2014 (RJ 658\2014 Giménez García) F.J. 1: «Es doctrina de la Sala que el principio de proporcionalidad, aunque no expresamente reconocido en la Constitución, debe ser considerado como el eje definidor de cualquier decisión judicial y singularmente de la individualización judicial de la pena que debe efectuarse teniendo en cuenta el grado o nivel de culpabilidad y la gravedad de los hechos, elementos que operan como la medida de la pena a imponer. SSTS 747/2007 ó 33/2013, entre las más recientes. A lo dicho debe añadirse que la Carta de Derechos Fundamentales de la Unión Europea, art. II-109 del Tratado VI, BOE de 21 de mayo 2005, reconoce expresamente el principio de proporcionalidad de los delitos y penas «....la intensidad de las penas no deberá ser desproporcionada en relación con la infracción....».

[24] Si atendemos a la Decisión Marco 2001/413/JAI del Consejo, del 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos al efectivo se caerá en la cuenta de que este precepto se introduce en el Código Penal como una obligación internacional para combatir tanto el fraude como la falsificación, pero ante

con los movimientos realizados mediante las tarjetas bancarias y otros mecanismos de pago?

Esta forma de protección empleada por el legislador no se ha visto libre de críticas. Prueba de ello es considerar ese precepto como un delito de sospecha, gramaticalmente se incrimina aquello que podría constituirse como la preparación de una posible defraudación sin que existan evidencias para demostrar el plan delictivo del sujeto[25] lo cual, abonaría a la infracción de la presunción de inocencia[26]. Sin embargo, podría defenderse la del «delito de programa de ordenador fraudulento» debido a la potencial capacidad que ostentan los programas informáticos a gran escala. Otro argumento para defender la legitimidad consiste en la dificultad de frenar la potencialidad criminal de los instrumentos, así como las exigencias de una sociedad en la que cada vez más le resulta indispensable el uso de cuentas bancarias y no pretende tolerar ninguna situación que resulte amenazante en ese lugar. En similar dirección, otro aspecto relevante consiste en la dificultad probatoria que caracteriza a la delincuencia informática[27].

Algunos proponen una interpretación restrictiva debido a la capacidad del programa informático, en ese orden, uno de los criterios restrictivos consistiría en limitar la aplicación del precepto cuando los programas sirvan exclusivamente para cometer defraudaciones informáticas[28]; es decir, no aplicar el tipo penal ante un programa de doble uso, pues el precepto señala que debe estar inequívocamente dirigido a la consumación de una defraudación; además, la elevación de la pena invitaría a exigir una interpretación restrictiva. Por otro lado, hay quienes opinan que es conveniente identificar la especificidad del programa y aunque se detecte otra utilidad, su principal función tendrá que ser la de conseguir una defraudación. Solo así se podría aplicar el precepto. Pero esta idea quizá no resulte convincente cuando un representativo grupo de programas tengan distintas capacidades (o funciones)[29].

Las propuestas señaladas son sugerentes, enriquecen el debate académico; pero, lamentablemente, no logran resolver todo el cúmulo de dificultades que caracterizan al delito de «programa de ordenador fraudulento». No se

---

todo para garantizar las formas de pago, con especial atención a las distintas al efectivo. Se analiza con detenimiento esa Decisión, se podrá ver que ni obliga ni sugiera castigar actos de preparación, no así las conductas de participación, instigación y tentativa; todas perfectamente aplicable con los respectivos dispositivos previstos en la Parte General del Código Penal.

[25] (Álvarez García, en Álvarez García, dir. 2011, 254-256). Quine muestra un análisis de este este delito como una evidente violación al principio de la presunción de inocencia.

[26] (Roxin y Schunemann 2019, 145-147).

[27] (Velasco Núñez y Sanchis Crespo 2019, 21-27).

[28] (Queralt Jiménez 2010, 520).

[29] (Gallego Soler en Corcoy Bidasola y Mir Puig, dirs., 2015, 554-555).

trata de una cuestión de presunción de inocencia, se requiere salvar exigencias igualmente relevantes como la lesividad, la proporcionalidad, la legalidad, o la intervención mínima. Por todo eso, urge que la incriminación logre integrarse con el sistema de Derecho Penal. Vamos a interpretar seguidamente las conductas incriminadas en el delito de «programa de ordenador fraudulento»[30].

III. VALORACIÓN DE LAS CONDUCTAS INCRIMINADAS

El «delito de programa de ordenador fraudulento», al ser un tipo alternativo se realiza por cualquiera de las varias opciones descritas[31]. En ese tipo se recogen cuatro modalidades.

Así pues, por fabricación entendemos creación del programa que posibilita la defraudación. Si se quiere optar por una interpretación restrictiva uno de los criterios para imputar la fabricación deberá ser la demostración de conocimientos técnicos por parte del acusado. Aunque el desarrollo de la tecnología avance a velocidades vertiginosas, el hecho de crear un programa de ordenador con la capacidad de defraudar no es algo que se encuentre al alcance de cualquiera. La expresión fabricar nos conduce a un acto de elaboración del programa. Esa voz puede ser interpretada de distintas maneras, pero casi nadie dudaría que solo después de la fabricación es posible introducir el programa, facilitarlo o poseerlo.

Por introducción entendemos la acción de instalar y dar funcionamiento al programa de ordenador, es decir, darle funcionalidad. Esta conducta puede ser realizada tanto por el creador como por otra persona[32], por ese molitivo se presentan problemas con el principio de culpabilidad, nadie puede responder por la acción criminal de otro.

Por posesión habrá que entender capacidad de disponer el programa, de ese modo, una posesión temporal y condicionada debe ser irrelevante; ya que el precepto señala con claridad que los programas deben estar específicamente destinados a la defraudación; y, por tanto, conviene seguir el siguiente criterio: gozar del programa de forma exclusiva y excluyente. No nos

[30] Véase, STC 3 de noviembre 2016 (RJ 229\2016 TC Pleno) F.J. 1.

[31] Véase, STS 26 de junio 2006 (RJ 692\2006 Sánchez Melgar) F.J. 5. A mi juicio, el legislador trata de evitar, como hemos afirmado, toda clase de supuestos delictivos para combatir la utilización de estos programas. El tipo también prohíbe la comercialización a partir de la prohibición de fabricar, como se sabe, es indispensable la preparación del programa para poder venderlo. Además, el precepto castiga la posesión sin importar los motivos que la hayan originado, pues no se comenta acerca de una indebida o injustificada posesión.

[32] (Álvarez García 2011, 255).

referimos a una necesaria relación física o directa, pues ello no es necesario en este concepto. Al tratarse de un programa para cometer un delito de estafa, no se puede hablar de posesión (delictiva) cuando se constituya una mera tenencia, esto es, tener el programa, pero sin la posibilidad de utilizarlo a falta de su instalación. Como adelantamos, ello no sería compatible con la exigencia de un programa «específicamente destinado a la realización de una defraudación». Piénsese, por ejemplo, en la persona que tiene el programa[33] en algún soporte magnético (o soporte de almacenamiento) sin que se encuentre instalado, para que la posesión sea relevante, a efectos de imputación, se requiere, al menos, un grado elevado de inmediatez y posibilidad en términos de uso (fraudulento)[34]. Lo contrario puede ocurrir cuando se requiera para su instalación de dos o más programas adicionales para determinar un funcionamiento. De este modo, el programa no reuniría las características concretas que constituyen un programa destinado a la comisión de una «estafa informática», pues lo que está *específicamente destinado* no puede estar al mismo tiempo «supeditado a la instalación de otro programa o inserción de otro artefacto» cuando se pretenda castigar por posesión. A nuestro parecer, destinado a la realización de una estafa, en atención a la pena asignada, así como a otras características del precepto, debería significar un paso previo e inmediato a la comisión de una defraudación. En ese orden, no pueden encontrarse trabas instrumentales respecto a la posesión de un programa que en términos penológicos se castiga exactamente igual que la consumación del delito fin (o tipo base).

Una de las conductas más interesantes es la denominada facilitación. Al respecto, podemos proponer dos interpretaciones del verbo facilitar. La primera, entenderlo como entregar o proporcionar algo a alguien. Así, la entrega del programa deberá ser idónea[35], es decir, el programa tendrá que estar en condiciones aptas para lograr la constitución de un riesgo típico, o sea, para alcanzar una transacción bancaria o una recopilación de datos (como números de tarjetas, contraseñas, nombres, correos, etc.) que hagan posible con posterioridad la defraudación. Pero la segunda acepción de facilitar

[33] Llegados a este punto es necesario aclarar un aspecto que tiene que ver con la responsabilidad penal. Pues es posible que el programa, en los términos arriba explicados, pertenezca a distintas personas o, en el *peor* de los casos, puede que el programa se encuentre a disposición de varios sujetos, o sea, que tengan capacidad de usarlos. De este modo, se reafirma que el aspecto fundamental en la tenencia no es otro que la disponibilidad potencial que puede ser imputable a varios sujetos, sin descuidar la posibilidad de dolo eventual en el caso de que varios sujetos gocen de dicha disponibilidad y uno de ellos sea sorprendido con el programa.

[34] (Pastor Muñoz 2005, 45).

[35] En sentido similar se muestra la STS 19 de noviembre 2014 (RJ 771\2014 Marchena Gómez) F.J. 4.

consistiría en hacer fácil o en hacer posible la ejecución de algo, esto es, ayudar a materializar un proyecto delictivo[36]. Sobre este particular, desde nuestro punto de vista, nos mostraría otra vía para la imputación que convierte en autor al cómplice, generando una extensión de la responsabilidad demasiado amplia, piénsese, por ejemplo, en la complicidad psíquica que extendería aún más el ámbito de aplicación de la norma[37].

El concepto de lesión se distancia del marco penal previsto en el art. 248.2 b). Podemos ver que en «el delito de programa de ordenador fraudulento» no es menester esperar a la lesión de un determinado bien jurídico para que se consuma. Hemos analizado brevemente las conductas incriminadas en esta norma, del mismo modo, recogimos algunos pronunciamientos doctrinales de cara a su aplicación; sin embargo, no hemos apuntado todavía las precisiones necesarias para responder cómo debería castigarse este delito. No podemos olvidar que el precepto objeto de estudio se presenta como un «acto preparatorio autónomo» distinto a los ampliamente conocidos actos preparatorios punibles[38] (arts. 17-18), esto genera no solo la necesidad de cotejar esta clase de preceptos con los «actos preparatorios punible», también nos invita a buscar una propuesta de solución, al menos, en el campo penológico.

IV. VALORACIÓN CRÍTICA

La conducta dolosa requiere la capacidad de realizar el tipo objetivo[39], nos referimos a los aspectos condicionantes que acompañan el ataque al bien jurídico[40]. El conocimiento de la situación debe ser incuestionable, es decir, el sujeto debe ser consciente que los programas tienen por objeto conseguir

[36] Comparten esta posibilidad, (Gallego Soler y Carlos Hortala Ibarra en Corcoy Bidasolo y Gómez Martín dirs. 2016 253-255).

[37] (Muñoz Conde y García Arán 2015, 477). Desde la definición de complicidad aportada por la doctrina, podemos pensar en un asesoramiento técnico; sin ir más lejos, cuando se le explica a alguien la forma más rápida y segura de utilizar el programa. También, cuando se le brinda asesoramiento para asegurar la impunidad del fraude. En todo caso, llama la atención que se pueda castigar como autor de un delito de estafa a quien lleve a cabo una conducta de complicidad (psíquica). En ese orden de asuntos, probablemente un sujeto que realice una estafa común recibirá una misma pena si lo comparamos con aquel que intente o, mejor dicho, colabore con la preparación de una defraudación informática sin que se produzca una disminución patrimonial en la cuenta bancaria de un tercero.

[38] Respecto a al a naturaleza excepcional de estas figuras, STS 22 de julio 2010 (RJ 335\2008 Berdugo Gómez de la Torre) F.J. 27.

[39] (Sánchez-Ostiz 2014, 115), quien entiende, entre otros, el dolo como conocimiento de la situación, admitiendo que la capacidad de controlar el estado generado por el sujeto se relaciona con su voluntad, voluntad que generalmente se incluye en el dolo.

[40] (Mir Puig, 2015, 179).

una defraudación; en otras palabras, el autor debe estar preparando, inequívocamente, una defraudación. A todo esto, debemos tener presente que la antijuridicidad del tipo debería estar revestida, por así decirlo, del injusto de la estafa básica, esto es así si se trata de una incriminación de un programa de ordenador para cometer una defraudación informática. No estamos ante la incriminación escueta de una posesión, fabricación, o facilitación, pues se castiga con pena privativa de libertad conductas que determinen la preparación de un injusto, igualando la preparación en el plano fenoménico a una estafa consumada. Dicho en otras palabras, el legislador ha elevado actos preparatorios a la categoría de delito, pero no a la categoría de estafa, porque en sentido fenoménico es imposible afirmar que existe una estafa. Casi nadie negaría que en el «delito de programa de ordenador fraudulento» se ausentan todos los elementos que constituyen el delito estafa.

Desde una interpretación literal el precepto se refiere a aquellos programas que tengan la específica finalidad delictiva, por ello sostenemos que los denominados programas de doble uso estarían excluidos de dicha literalidad. Así, si se mantiene la pena vigente y se demuestra que un programa tiene otra finalidad, el precepto no debería aplicarse (a no ser que la posesión del programa se vea acompañada de otros elementos que determinen de manera inequívoca la preparación de una estafa informática). Esto se reafirma al tratarse de figuras excepcionales, pues no es normal que en la legislación española se castiguen actos de preparación de amanera autónoma en la Parte Especial. Si bien el «delito de programa de ordenador fraudulento» no es un «acto preparatorio punible»[41], ello no significa que la incriminación de esas conductas preparatorias escapen del marco de la excepcionalidad y la excepcionalidad exige una valoración particularizada que derive hacia una oportuna imputación, rechazando que puedan aplicarse esta clase de normas relajando los estándares establecidos.

Más allá de los verbos típicos comentados, es decir, de cualquiera de las alternativas contenidas en el precepto, también es posible dar un paso más, esto es, lograr la producción del resultado mediante la utilización de los programas: conseguir una trasferencia o facilitar el instrumento para que otro sujeto materialice una defraudación. También es posible que el sujeto inicie el proceso de defraudación sin que lo consiga por causas ajenas a su voluntad. De modo que se produciría una tentativa de estafa, aunque no se haya lesionado el patrimonio. En similar sentido, si se consigue lesionar el patrimonio de otro, deberá aplicarse únicamente la pena del delito consumando por tratarse de un concurso de leyes[42]. Vemos entonces, como indicamos, que

[41] Para una exposición histórica de la regulación de los actos preparatorios punibles en la legislación española, véase (Mir Puig, 2015, 350-353).

[42] (Dopico Gómez-Aller, 2018, 230-231).

se corresponde con una indiscutible sobreprotección penal para el patrimonio económico. Ahora bien, respecto a la aplicación de la sanción, son interesantes los criterios que se recogen en el precepto contenido en el art. 249, describe algunas pautas de cara a la fijación de la pena, en ese precepto aparece un conjunto de criterios como el importe de lo defraudado, el quebranto económico, entre otros. Sin embargo, el «delito de programa de ordenador fraudulento», de conformidad con su naturaleza instrumental, no permite determinar el importe de lo defraudado; y no puede admitirse la aplicación de un cálculo hipotético o presunto respecto a la defraudación; esto desbordaría todas las garantías que emanan del principio de legalidad[43]. El art. 249 brinda cinco criterios; estos no se refieren, únicamente, al importe de lo defraudado y al quebranto económico causado, también aparecen otros como «las relaciones entre el sujeto activo pasivo, los medios empleados por el sujeto activo y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción». Como puede verse, de todos los criterios citados, los dos últimos son los que podría emplear el operador judicial para sancionar el «delito de programa de ordenador fraudulento». Piénsese, por ejemplo, en la tenencia de un programa en óptimas condiciones, esto es, perfectamente instalado para conseguir una disminución patrimonial, pero además, acompañado de una lista donde reposan los nombres de varios clientes de un banco junto a sus correos electrónicos (información aportada por un empleado de la entidad). Al mismo tiempo, supóngase que se trata de una lista con criterios inequívocamente delictivos, pongo por caso, clientes con solvencia económica y de la tercera edad[44], de modo que sea menos probable la reacción inmediata (o posterior) de la víctima de cara a la defensión.

[43] Es bastamente conocido que en Derecho penal rechazamos las presunciones *juris et de jure,* en nuestro caso, aquellas que sirven para considerar que habrá o que hay una lesión cuando en realidad no la hay. A mi modo de ver, esta clase de criterios son constitucionalmente inaceptables, pues se basan en tipificaciones que carecen de lesividad, construyendo sus bases sistemáticas en presunciones ofesividad.

[44] El supuesto planteado es posible bajo el género «página web o ventana emergente», probablemente sea la estrategia más utilizada en este ámbito delictivo. El método es el siguiente, se envía un correo electrónico a los clientes suplantando la identidad del banco, pero al correo que el titular de la cuenta reportó en la entidad bancaria. La finalidad del correo es facilitar datos bajo cualquier excusa, por ejemplo, para actualizar la base de datos del banco o confirmar una transacción. De este modo se logra obtener el número de la tarjeta de crédito o débito, el CVV o código valor de verificación o validación que se encuentran en el reverso, así como la fecha de caducidad y otros datos necesarios para realizar una compra en Internet. Nótese, de momento, que para conseguir este fraude no es necesario la tenencia de un programa que sirve únicamente para conseguir una estafa, criterio interpretativo restrictivo que sostienen algunos. Pues como vemos, en la artimaña entran en juego factores como la apariencia de veracidad del correo y la inocencia del cliente.

En un caso como el citado, casi nadie negaría la creación de un riesgo típicamente relevante de cara a una preparación para el delito de «defraudación (o estafa) informática»; sin embargo, no podemos negar que continuamos en un estado de preparación pura. Por otro lado, al tratarse de sistemas y programas informáticos, la experiencia ha demostrado que se pueden producir problemas técnicos ajenos a la voluntad del preparador, impidiendo la ejecución de la trasferencia o la recopilación de los datos para realizar una defraudación *a posteriori*; no así la tentativa del «delito de programa de ordenador fraudulento» o, dependiendo de las circunstancias concretas que acompañen la tenencia, «una consumación del delito de programa de ordenador fraudulento».

La excepcionalidad que caracteriza al «delito de programa de ordenador fraudulento» amerita una interpretación restrictiva para posibilitar su permanencia en el Código Penal, de lo contrario, la aplicación de la norma implicaría un despropósito. Dicho esto, vamos a presentar nuestra propuesta de reforma que intenta cubrir las garantías mínimas del delincuente.

V. REFLEXIÓN FINAL Y PROPUESTA DE *LEGE FERENDA*

El «delito de programas de ordenador fraudulento» presenta una controvertida extensión de la responsabilidad penal que obstaculiza la aplicación de los esquemas clásicos de imputación. Esto hace que se requieran criterios específicos para logar una aplicación acorde con los principios básicos del Derecho penal.

Las soluciones aparentemente definitivas que recogimos en esta investigación no logran resolver todos los inconvenientes de esta controvertida norma. Derogar el precepto implicaría negar la voluntad del legislador de prohibir la existencia de programas con capacidad delictiva que afectan a los ciudadanos. Si bien el legislador –en el marco de sus facultades– cuenta con la potestad de castigar las conductas que estime indeseadas, no puede desprenderse de los principios constitucionales, entendiendo que el Derecho penal, a pesar de su *tocante* autonomía, es un apéndice del Derecho Constitucional, está sometido a la ley fundamental[45], este sometimiento deriva de

[A]demás del supuesto planteado, aunque más complejo, sería la estafa masiva, pero a mínima escala. Esto es, defraudar en pequeñas cantidades; por ejemplo, de uno a tres euros, pero en miles de cuentas bancarias. De este modo, se lograría un gran incremento patrimonial injustificado y las posibilidades de sospechas disminuyen en comparación con una defraudación que supera las cantidades citadas.

[45] (Zaffaroni 2011, 37).

[A]demás del supuesto planteado, aunque más complejo, sería la estafa masiva, pero a mínima escala. Esto es, defraudar en pequeñas cantidades; por ejemplo, de

una función protectora del Estado como titular de los bienes jurídicos reconocidos en el sistema. No en vano, se habla del sometimiento de los poderes públicos al Derecho, esto es, de un sometimiento a la Constitución, que, como es de sobra conocido, dicha Norma goza de un distrito preponderante en el sistema jurídico (art. 9 CE).

Una de las propuestas más comentadas se refiere a la aplicación del precepto cuando los programas sirvan, exclusivamente, para realizar estafas masivas, pero esa fórmula no logra abarcar toda la problemática que envuelven al precepto, porque no siempre se tratará de estafas masivas; ya vimos que con la norma se intenta proteger no a un grupo determinado de sujetos privilegiados, sino a cualquier ciudadano; al mismo tiempo, tampoco resuelve otro de los problemas fundamentales: la desproporcionalidad.

De todos los aspectos controvertidos, el más relevante es el tratamiento penológico; por ese motivo centramos nuestra investigación en una propuesta de reforma que pueda servir no solo para el sistema español; también para legislaciones cercanas que no tengan esta norma en su código y pretendan sancionar la preparación para la defraudación informática. Sancionar actos de preparación con la misma pena prevista para la realización perfecta del delito fin (o tipo base) sobrepasa los límites del poder punitivo del Estado, pues se equipara, en términos criminológicos, la preparación delictiva con la materialización del tipo base. Como es de sobra conocido, se trata de una decisión ilegítima en un Derecho penal respetuoso de los postulados que rigen un Estado Social y Democrático de Derecho: no es lo mismo la capacidad de lesionar que la lesión; en otras palabras, no es lo mismo la potencialidad de cometer un delito de estafa que cometer una defraudación; como tampoco es igual planificar la comisión de un robo que intentarlo. Sin embargo, el legislador se empeña en castigar actos de preparación con la misma pena prevista para la consumación del delito fin[46]. Desde nuestra posición, esta clase de decisiones nos muestran un elevado grado de irracionalidad punitiva; por lo cual nos restaría, en estas páginas, proponer alternativas que se muestren alejadas de la arbitrariedad legislativa y se acerquen a las garantías constitucionales.

La propuesta penológica que hemos preparado para el delito de «programa de ordenador fraudulento» es la siguiente:

> *«Art. 248.3 Los que fabricaren, introdujeren o facilitaren programas informáticos, acompañados de otros elementos inequívocamente predesti-*

uno a tres euros, pero en miles de cuentas bancarias. De este modo, se lograría un gran incremento patrimonial injustificado y las posibilidades de sospechas disminuyen en comparación con una defraudación que supera las cantidades citadas.

[46] Respecto a la irracionalidad legislativa, véase la interesante aportación de (Zaffaroni 2006, 746).

nados a la realización de defraudaciones informáticas previstas en este código serán sancionados con una pena de multa de seis a veinticuatro meses».

Nuestra propuesta, que incluye una pena de multa, obedece, en mayor o menor medida, al grado de peligro que representen los aparatos para el patrimonio económico de los ciudadanos. Una sanción que está inspirada en el grado de peligrosidad de los aparatos, siempre que se encuentren acompañados de un conjunto de materiales que determinen la univocidad fraudulenta respeta la presunción de incendia. En esa línea, el precepto se acercaría mucho más a las garantías del sujeto, eliminando la posibilidad de hacer responsable a alguien por la conducta de otro; excluyendo la posibilidad de incriminar la mera posesión de aparatos; reduciendo el ámbito de aplicación a la estafa informática. En otro precepto del mismo Código Penal se incrimina la simple tenencia de cosas aunque estas se encuentren ocultas, bajo llave o, inaccesibles, casi nadie refuta su castigo… Me refiero a la tenencia de armas prohibidas o tenencia ilícita de armas (art. 563 CP). Esa norma establece una pena de prisión de uno a tres años, casi nadie discute la sanción. Como se mencionó, la discusión es casi nula, posiblemente no tanto por la elevada potencialidad que representan las armas, sino por la clase de bienes jurídicos que con ellas se pueden lesionar. Con todo, estas representan una relevante anticipación de las barreras de protección. Mientras que en el otro lado de la balanza, vimos que la prohibición de objetos o instrumentos idóneos para facilitar la comisión de una defraudación en el ámbito informático podría parecer acertada debido a la complejidad que representan para las potenciales víctimas; no obstante, la redacción del precepto –incluyendo la sanción– es inadecuada porque desatiende los principios básicos del Derecho penal, por eso es necesaria una modificación, para lograr que la medida legislativa sea valorada como Política.

En un Estado social y democrático de Derecho, una de las características esenciales es la armonización de la pena. Pero otra característica es el respeto de todos los principios limitadores del poder punitivo del Estado durante el proceso legislativo que incluye las normas. Igualmente, la propia Constitución exige que se brinden garantías cuando nos referimos al Derecho penal, entre otras razones, por tratarse de la vía más drástica para defender los bienes jurídicos del Estado. En tal orden, acudir al Derecho penal implica una programación mesurada al momento de incriminar conductas y proponer penas. Cuando se decide incriminar acciones que se estimen reprochables, en nuestro supuesto, cuando considera reos de estafa a quienes «fabriquen, introduzcan, posean o faciliten programas informáticos específicamente destinados a la comisión de las estafas»; deben preverse las divergencias entre los grupos de delitos que se contienen en el Código Penal con las penas previstas dependiendo de los bienes jurídicos que se lesionen, así como otras

circunstancias que justifican el grado de la sanción como ocurre con los denominados *delitos cualificados por el resultado*. En ese sentido, se requiere que la redacción del precepto no solo sea flexible con las conductas incriminadas, sino que, además, la incriminación se corresponda con los fines preventivos tanto generales como especiales orientados al control social.

Para cerrar, es necesario no solo que la incriminación de las conductas garantice su evitación, también la compatibilidad de la norma con los principios constitucionales, y esto incluye, en un plano de elevada importancia, la sanción, pues esta pretende, conforme a un determinado plan, dirigir, desarrollar o modificar el orden social.

VI.CONCLUSIONES

En el delito de «programa de ordenador fraudulento», en ningún período de la actividad preparatoria envuelve una lesión en sentido fenoménico, tampoco se aprecia una afectación mínima, de ahí se derivan los problemas de constitucionalidad. En contraposición, existen actos preparatorios que, durante su periodo, plasman –de manera inobjetable– una pluralidad de acciones lesivas en virtud de la naturaleza del delito pretendido. Nos referimos a delitos como la rebelión o la sedición. En esas infracciones penales, durante su complejo desarrollo de preparación se afectan diferentes bienes jurídicos (revelando secretos, amenazando sujetos, poseyendo o compadrando armamento ilícito…). El adelantamiento de la intervención se admite, de manera excepcional, porque al conseguirse el proyecto delictivo sería imposible «devolver las cosas» a su estado anterior (seguridad interior del Estado, cambio de régimen Constitucional…). Dos criterios que respaldan la excepcionalidad: (i) relevancia del bien jurídico protegido; (ii) y necesaria afectación a otros intereses desde el curso de la preparación. Sin embargo, estos criterios se ausentan en el «delito de programa de ordenador fraudulento», por tanto, no debería admitirse esta clase de anticipación, bastando la protección del delito fin o tipo base, esto es, el delito de fraude informático. Pero si se admite, por lo menos, la sanción debe flexibilizarse al grado de «puesta en peligro o lesión».

La pena descrita en el precepto contenido en el art. 248.2 b) del Código Penal, debe ser rechazada. Mediante nuestra propuesta de reforma se contempla la posibilidad de cambiar radicalmente la norma sin que se pierdan las garantías que el legislador pretende ofrecer a la ciudadanía. A nuestro juicio, parece mucho más razonable aplicar una pena de multa, dado que se corresponde mucho más con la aparente «puesta en peligro o lesión». Conjuntamente, la propuesta que presentamos limita el alcance a las denominadas «estafas informáticas», excluye la sanción para los programas de doble uso,

deroga el castigo por mera posesión, y emite una pauta general de interpretación, ya que demanda que los programas se encuentren, inequívocamente, predestinados a una defraudación.

El precepto contenido en el art. 248.2 b) del Código Penal no debe ser considerado como un modelo de aplicación para otras latitudes. Si bien la medida adoptada por el legislador puedo estar «dotada de buenos propósitos», peca por excesiva, y es excesiva porque abandona nociones fundamentales como resultado, peligrosidad, lesividad. En consecuencia, desarma al ciudadano de sus garantías. Inadmisible resulta entonces sancionar manifestaciones de voluntad en las que no se visualizan en sentido fenoménico ni siquiera en un mínimo lo que criminológicamente denominamos «el paso al hecho delictivo».

BIBLIOGRAFÍA

Aboso, Gustavo y Zapata, María. 2006. *Cibercriminaldiad y Derecho penal.* Montevideo, Buenos Aires: BdeF.

Álvarez García, Francisco Javier, en Álvarez García, Francisco Javier dir. 2011. *Derecho penal español. Parte especial,* Tomo 2. Valencia: Tirant lo Blanch.

Anarte Borrallo, Enrique y Doval Pais, Antonio en Boix Reig, Javier dir. 2012. *Derecho penal. Parte Especial,* Vol. 2. Madrid: Iustel.

Cruz de Pablo, Antonio José. 2006. *Derecho penal y nuevas tecnologías: Aspectos sustantivos: adaptado a la reforma operada en el Código Penal por ley orgánica 15/2003 de 25 de noviembre, especial referencia al nuevo artículo 286* CP. Madrid: Grupo Difusión.

Dopico Gómez-Aller, Jacobo *et. al.* 2018. *Derecho penal económico y de la empresa.* Madrid: Dykinson.

Faraldo Cabana, Patricia. 2006. *Las nuevas tecnologías en los delitos contra el patrimonio*. Valencia: Tirant lo Blanch.

Gallego Soler, Ignacio y Hortala Ibarra, Juan Carlos, en Corcoy Bidasolo, Mirentxu y Gómez Martín, Víctor dirs. 2016. *Manual de Derecho penal, económico y de empresa. Parte General y Parte Especial (adaptado a las LLOO 1/2015 y 2/2015 de Reforma del Código Penal). Doctrina y jurisprudencia con casos solucionados,* Tomo 2. Valencia: Tirant lo Blanch.

Gallego Soler, Ignacio, en Corcoy Bidasola, Mirentxu y Mir Puig, Santiago dirs. 2015. *Comentarios al Código Penal.* Valencia: Tirant lo Blanch.

Mir Puig, Santiago. 2015. *Derecho Penal. Parte General,* 10.ª ed. Reppertor: Barcelona.

Muñoz Conde, Francisco. 2019. *Derecho Penal. Parte Especial.* Valencia: Tirant lo Blanch.

Pastor Muñoz, Nuria. 2005. *Los delitos de posesión y los delitos de estatus Una aproximación político-criminal y dogmática.* Barcelona: Atelier.

Queralt Jiménez, Joan. 2010. *Derecho Penal español. Parte Especial,* 6.ª ed. Barcelona: Atelier.

Romeo Casabona, Carlos, en Romeo Casabona, Carlos y Boldova Pasamar, Miguel coords. 2016. *Derecho penal. Parte especial.* Granada: Comares.

Roxin, Claus y Schunemann, Berns. 2019. *Derecho procela penal,* 29. ª ed. Buenos Aires: Ditod.

Roxin, Claus. 1981. «Culpabilidad, prevención y responsabilidad en Derecho Penal», en *Culpabilidad y prevención en Derecho Penal.* Madrid: Reus.

Sánchez-Ostiz, Pablo. 2014. «En qué medida imputa y es objetiva la «imputación objetiva»», en *La libertad del Derecho penal. Estudios sobre la doctrina de la imputación.* Barcelona: Atelier.

Silva Sánchez, Jesús. 2012. *Aproximación al Derecho penal contemporáneo,* 2.ª ed. Montevideo/Buenos Aires: BdeF.

Tavares, Juarez. 2010. *Teoría del injusto penal.* Montevideo/Buenos Aires: Bdef.

Velasco Núñez, Eloy y Crespo, Carolina Sanchis. 2019. *Delincuencia Informática. Tipos Delictivos e Investigación Con Jurisprudencia tras la Reforma Procesal y Penal De 2015.* Valencia: Tirant lo Blanch.

Zaffaroni, Eugenio Raúl, *et. al.* 2006. *Manual de Derecho Penal. Parte General.* Buenos Aires: Ediar.

—— 2011. *Estructura básica del Derecho penal.* Buenos Aires.

LA PENALIDAD DEL DELITO DE PROGRAMA DE ORDENADOR FRAUDULENTO EN EL CÓDIGO PENAL ESPAÑOL. RÉGIMEN VIGENTE Y POSIBILIDADES DE REFORMA

The penalty of the crime of fraudulent computer program in the spanish penal code. current situation and possibilities for reform

Roberto Cruz Palmera
Doctor en Derecho. Profesor de Derecho Penal
Universidad Autónoma del Caribe (Barranquilla, Colombia)
rcruz.3@alumni.unav.es

http://dx.doi.org/10.18543/ed-68(2)-2020pp75-95