Posada, R. (2017). *Los cibercrímenes: un nuevo paradigma de criminalidad. Un estudio del Título VII bis del Código penal.* Bogotá: Universidad de los Andes-Ibáñez, 482 pp.

Juan David Jaramillo Restrepo[*]

El libro objeto de la presente reseña fue elaborado por el Profesor Ricardo Posada Maya, Director del Área de Derecho Penal, Procesal Penal y Criminología de la Universidad de los Andes (Bogotá, Colombia), y cuenta con el prólogo de la Profesora Laura Zúñiga Rodríguez y ha sido dedicado a su «maestro, Fernando Velásquez Velásquez, con el aprecio y la admiración de siempre». El trabajo se divide en cinco partes: en la primera, se presenta la obra (pp. 15-17); en la segunda, se realiza «una aproximación a los delitos informáticos» (pp. 33-161); en la tercera se estudian, en particular, «los cibercrímenes en Colombia» (pp. 165-439); en la cuarta se consignan las conclusiones (pp. 441-482); y, en la quinta, se recogen las fuentes de información (pp. 453-482).

Para comenzar con la «Presentación» debe decirse que el libro de investigación, en palabras del autor, «plantea toda una teoría general del delito informático (en sentido amplio y estricto), y un estudio minucioso de la parte especial (Ley 1273 de 2009), en el que se analizan las diversas figuras criminales incorporadas a la legislación penal nacional y sus reformas» (p. 17). Es un texto académico «que pretende convertirse en una fuente de investigación y consulta técnica muy documentada y problematizada, de vital importancia para los estudiantes de derecho, los jueces, fiscales y, en general, para todos aquellos que se dedican al estudio de esta disciplina. Todo esto de acuerdo

[*] Abogado, Maestro en Derecho, Profesor de Derecho Penal Especial de la Universidad Sergio Arboleda y miembro del grupo de Investigación en Ciencias Penales y Criminologicas «Emiro Sandoval Huertas». Correo: juan.jaramillo@usa.edu.co.

con la perspectiva político-criminal que exige el modelo de Estado social y democrático de Derecho» (p. 17).

Cuando se hace «Una aproximación a los delitos informáticos», se delimita el objeto de estudio. La idea central que rige la estructura es la siguiente: Inmerso en el nuevo paradigma de la cibercriminalidad (en donde pululan riesgos informáticos de diversa índole) (pp. 33-97), y en el marco de los más recientes instrumentos internacional (por ejemplo, el Convenio de Budapest) (pp. 141-143), el Derecho penal nacional intenta proteger el bien jurídico autónomo y *sui generis* de la seguridad de la información y de los sistemas informáticos mediante la creación de nuevos delitos que se orientan a salvaguardar objetos especiales de tutela (datos informáticos, información informática, sistemas operativos y sistemas informáticos) (pp. 113-139), aunque, por la constante evolución de la tecnología, siempre se encuentra a la «zaga de la impunidad» y no logra castigar todos los comportamientos nocivos (v. g., el *cyberstalking,* el *ciberbullying* o la *falsedad informática*) (pp. 145-161).

Al examinar «Los cibercrímenes en Colombia», su autor se adentra en la estructura de los comportamientos castigados en la Parte Especial del Código Penal colombiano, agrupándolos en cuatro grupos. Primero: los delitos de intrusismo (el *acceso abusivo a un sistema informático*, art. 269A) (pp. 233-269); el segundo: los delitos de espionaje (*interceptación de datos informáticos*, art. 269C; *violación de datos personales*, art. 269F; y *suplantación de sitio web para capturar datos personales*, art. 269G) (pp. 271-327); el tercero: los delitos de sabotaje (*obstaculización ilegítima de sistema informático o red de telecomunicación*, art. 269B; *daño informático*, art. 269D; y *uso de software malicioso*, art. 269E) (pp. 329-374). Y, el cuarto: los delitos de defraudación informática (*hurto por medios informáticos y semejantes*, art. 269I; *transferencia no consentida de activos*, art. 269J, inc. 1; y *fabricación, posesión, introducción y facilitación de software defraudatorio*, art. 269J, inc. 2) (pp. 375-421). Al final, el lector encuentra un breve estudio del delito de *manipulación de equipos terminales móviles* (art. 105 de la L. 1153/2011) y de las *circunstancias de agravació*n del Título VII bis (art. 269 H, C. P.).

Así mismo, en las «Conclusiones» se pone de presente que las ideas más importantes del libro son las siguientes: a) el paradigma de la cibercriminalidad hace parte de la política criminal del nuevo derecho penal (p. 441); b) los avances informáticos y telemáticos han generado el surgimiento de nuevos riesgos digitales masivos, transnacionales e internacionales, especializados, automáticos, invisibles, continuos y anónimos (pp. 442-444); c) en este campo, se deben distinguir los cibercrímenes (delitos propiamente informáticos) de los delitos vinculados a la red (delitos cometidos por medios informáticos) (p. 446); d) la Ley 1273 de 2009 es una inequívoca expresión jurídica de la evolución social de un mundo interconectado e internacional (p. 441). Así mismo: e) la legislación vigente ha creado un nuevo bien jurídico autónomo, intermedio o de referente individual que se concreta en la seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos (pp. 446-447); f) los bloques de criminalidad informática son el intrusismo, el espionaje, el sabotaje y las defraudaciones informáticas (pp. 448-449); g) es necesario reestructurar algunas figuras criminales previstas en el Código Penal y crear otras nuevas (pp. 444-446); y, h) el cambio virtual ha motivado profundas transformaciones en el derecho penal (en temas como el nexo de causalidad, la imprudencia, la omisión, etc.) (pp. 450-451).

En lo atinente a la bibliografía se destaca la muy amplia lista de referencias (compuesta por más de cuatrocientas entradas) que agota los autores colombianos y extranjeros más consultados en nuestro medio. Lo anterior, advirtiendo que, en el ámbito nacional, nos encontramos en un terreno prácticamente inexplorado (técnico, complejo y especializado), en donde la doctrina es escasa y no abunda la jurisprudencia.

De igual forma, no sobra recordar que este libro es el resultado de un proceso de reflexión que comenzó hace más de diez años con el artículo «Aproximación a la criminalidad informática» (2006) y se consolidó progresivamente con otros estudios: «¿Es integral la protección jurídico penal por intrusión informática para titulares de información reservada?» (2006); «El derecho penal de la globalización *vs.* el Derecho penal de la globalización alternativa» (2009); «El delito de transferencia no consentida de activos» (2012);

«El delito de acceso abusivo a sistema informático» (2013); e «Interceptación informática y violación de datos personales» (2016). El punto final se escribió en una estancia postdoctoral de investigación en la Universidad de Salamanca, España.

En fin, se debe destacar la importancia de este aporte llamado a agitar la discusión en un campo necesitado de reflexiones a profundidad como la que hace Posada Maya quien, por supuesto, con esta investigación se consolida como uno de los más granados exponentes de la doctrina nacional que, por supuesto, acoge con plácemes este tipo de incursiones académicas. El texto, pues, se convierte en obligado material de estudio para quienes aborden el título VII Bis de la Parte Especial de nuestro Código Penal y se torna, además, en punto de referencia para las necesarias transformaciones legislativas que se requieren.