Reseña sobre el libro *"Delitos informáticos. Investigación criminal, marco legal y peritaje"* de Gustavo Sain y Horacio Azzolin.

Por Marcelo Riquert*

"Delitos informáticos. Investigación criminal, marco legal y peritaje" de **Gustavo Sain y Horacio Azzolin**. Prólogo del Dr. Carlos M. González Guerra. Serie Criminalística, dirigida por Carlos A. Guzmán y María Fernanda Ferreyro. Ed. BdeF, Montevideo-Buenos Aires, 2017, 202 págs.

Esta obra es el producto de la interactuación de profesionales de distintas áreas que confluyen sobre un tema de común interés. Gustavo Sain es Licenciado en Ciencias de la Comunicación y Magíster en Sociología y Ciencias Políticas que se desempeña como asesor especialista en cibercrimen en la Dirección Nacional de Política Criminal del Ministerio de Justicia y Derechos Humanos de la Nación. Horacio Azzolin es Fiscal Federal con larga trayectoria en el servicio de justicia, desde fines de 2015 jefe de la Unidad Fiscal Especializada en Ciberdelincuencia. Este sólo dato es auspicioso: estamos frente a un trabajo presidido por la noción de interdisciplina, tan necesaria como habitualmente olvidada según predicaba el querido maestro, Prof. Dr. David Baigún.

Los aportes de Sain se concentran en el primero y cuarto capítulos: "Internet, el cibercrimen y la investigación criminal de delitos informáticos" y "Dificultades del proceso judicial en la investigación de delitos relacionados con dispositivos informáticos". En el inicial nos proporciona información de suma importancia para la adecuada comprensión del contexto en que la delincuencia informática se despliega. Así, las nociones/conceptos de dispositivo informático, internet y su gobierno, redes y delito informático. Luego, transita otras menos frecuentadas en la bibliografía nacional y avanza sobre la informática forense y la evidencia digital, la escena del crimen y el modo en que debiera configurarse un equipo de investigación eficaz en esta materia. En el otro, comienza plateando las dificultades generales que tiene el derecho para aprehender la fenomenología informática, dando paso después al abordaje de tópicos concretos donde podría decirse que la nota de originalidad está dada porque se privilegia la perspectiva práctica por sobre la jurídica. Así, se suceden

cuestiones como la territorialidad, jurisdicción y competencia territorial, la admisibilidad de la prueba en el proceso penal, la responsabilidad legal de las empresas proveedoras de servicios de Internet y las políticas públicas para la red.

Por su parte, Azzolin aporta el segundo capítulo "Una aproximación a la evidencia digital: tratamiento, adquisición y preservación" (junto a Nicolás Bru) y el tercero "El marco legal de los delitos informáticos" (junto a Belén Ravarini y, de nuevo, Nicolás Bru). El primer aporte es una suerte de continuidad con el capítulo inicial ya que profundiza consideraciones relativas a qué ha de entenderse por evidencia digital, cuáles son las fases en que puede dividirse el proceso informático forense y, muy importante en tanto se carece de regulación procesal vigente, acerca de cuáles serían los procedimientos apropiados para la adquisición y preservación de la prueba. El segmento siguiente es el que tiene un mayor contenido jurídico dogmático, siendo donde se concreta primero una suerte de estado de situación de la normativa legal vigente en materia fondal y, luego, adjetiva en nuestro país. Así, rápidamente se pasa una mirada sobre la actual tipificación penal y las pocas normas del CPPN (cf. ley 23984) que tienen vinculación con la cuestión informática. Este capítulo finaliza con un comentario sobre el marco legal internacional que plasma en un análisis sobre el Convenio de Budapest de 2001.

Se han incorporado dos "Anexos". El primero con un muy interesante estudio concretado por la citada DN de Política Criminal titulado "Una aproximación a la estadística criminal sobre delitos informáticos: primer muestreo de denuncias judiciales de la República Argentina", comentado por Gustavo Sain, que nos permite conocer estadísticas sobre delitos informáticos previstos en la ley 26388 (de reforma del CP) entre los años 2012/2013 tanto a nivel nacional como, con mayor detalle, en la CABA y en la provincia de Buenos Aires. Es de esperar que este trabajo se mantenga y profundice cubriendo la recolección estadística con frecuencia anual y hasta la actualidad. Sobre todo porque estamos frente a un fenómeno expansivo cuyo crecimiento no debiera seguir necesariamente la evolución de la estadística criminal general. El condicional se impone porque, justamente, la carencia de datos específicos y la reflexión sobre su significancia campean por su ausencia.

Lo que no puede soslayarse es que el factor tecnológico se extiende hasta cubrir insospechados intersticios de nuestro quehacer diario y esa suerte de omnipresencia provoca que sea medio u objeto de conductas disvaliosas en forma cada vez más frecuente. Así, por dar un ejemplo, puede advertirse el modo en que en segmentos de

delitos como las defraudaciones el ardid o el engaño presencial va siendo desplazado por la manipulación informática en un mundo donde tanto la economía "analógica", la del dinero en efectivo, y el ofrecimiento de servicios en forma personal son paulatina pero rápidamente reemplazados por la economía "digital", la de la banca electrónica, y los servicios "online". Si se consulta la bibliografía especializada en España en torno al fraude informático, debido a la crisis de comienzo de década, los juzgados se poblaron de causas contra los denominados "cibermuleros" y es común en la doctrina leer que, en aquél momento, era más fácil encontrar fallos sobre defraudación por phishing que por una estafa tradicional. Tal vez, una exageración. Sin duda, una tendencia.

El segundo anexo, por cierto, útil pero de menor interés es relativo a la "Legislación relacionada" y reúne una serie de instrumentos normativos, a saber, las leyes 26388 (delitos informáticos), 26904 (grooming) y 25326 (protección de datos personales) y, por último, el texto en español del Convenio sobre ciberdelito de Budapest (2001).

Puede agregarse que, más allá de la división de trabajo, la visión de unidad del texto no ha sido perdida de vista y que si bien los capítulos son de autoría individual o plural diversa mantienen una suerte de hilo conductor, se complementan y no se advierten innecesarias reiteraciones. En suma, debe coincidirse con el distinguido prologuista, Dr. González Guerra, cuando concluye que estamos frente a una obra cuyo interés no sólo es para el especialista sino también para el público en general que quiera conocer y comprender sobre la problemática de la ciberdelincuencia en nuestro país.

Universidad Nacional de Mar Del Plata (UNMD)