PRÓLOGO

El nuevo milenio ha traído consigo un cambio trascendental en la relación de las personas con las Tecnologías de la Información y la Comunicación (TICs). En especial la tecnología informática —cuyo uso, hasta fines del siglo pasado, estaba reservado a un sector minoritario que contaba con los conocimientos necesarios— se ha tornado ubicua, y forma parte de la vida diaria de la mayor parte de la población del planeta. La expansión de la Internet, de la computación personal y de los teléfonos inteligentes, ha generado que prácticamente todas las actividades humanas se lleven a cabo o estén conectadas con algún dispositivo informático.

Las personas recurren a estos dispositivos para informarse, para ubicarse, para comunicarse, para estudiar, para trabajar, para entretenerse y —por supuesto— también para delinquir. En efecto, la revolución tecnológica que estamos viviendo no solo ha dado a luz a nuevos delitos, producto de las características de este nuevo ecosistema virtual (como el *ramsonware* o la intrusión informática), sino que muchos delitos propios del mundo físico como la extorsión, el lavado de activos, la difusión de imágenes de explotación sexual infantil y hasta la violencia de género, han encontrado un terreno fértil para desarrollarse en el ciberespacio.

Por añadidura, el hecho de que la tecnología informática se haya colado en (casi) todos los aspectos de la vida diaria de las personas, deriva en la generación de un volumen casi inabarcable de información digital sobre los ciudadanos, la cual puede —por supuesto— servir como prueba en el marco de los procesos penales vinculados no solo a los ciberdelitos propiamente dichos, sino de cualquier delito en general. Esta evidencia digital presenta, sin embargo, características propias que la distinguen de la evidencia "física" habitualmente utilizada para probar la comisión de los delitos "tradicionales", toda vez que se trata de datos informáticos de alta volatilidad, muy fáciles de copiar, alterar o destruir, y que requieren de herramientas específicas para su percepción, recolección y análisis.

En este escenario, los agentes de las fuerzas de seguridad, peritos, fiscales, abogados defensores y jueces, los legisladores e incluso el público en general (si preten-

de evitar ser víctima de estos delitos), están obligados a adaptarse a la nueva realidad generada por la evolución tecnológica, cuyo continuo avance, además, no deja margen para un aprendizaje lento o paulatino. Y aunque en los últimos años, la oferta de información y capacitación para la mayoría de estos actores ha aumentado en forma exponencial, es evidente que ningún país del mundo —y mucho menos la Argentina— está en condiciones de capacitar a todos los operadores del sistema en lo inmediato.

Es en este contexto en que se vuelven invaluables obras de difusión como las que nos ofrece Lucas Moyano con este nuevo libro. Un autor que, a pesar de su juventud, cuenta con una extensa experiencia en el campo de la investigación y persecución de los ciberdelitos, y presenta un trabajo dirigido a quienes se encuentran en el frente de batalla, escrito desde el frente de batalla, ideal para servir como puerta de entrada a esta nueva realidad para todos aquellos que la miran desde afuera, algo perplejos.

La presentación de una temática compleja como es la investigación de delitos en el entorno digital, cuando está dirigida a los no iniciados, demanda que se balancee la necesidad de transmitir el conocimiento de todos los aspectos técnicos requeridos para poder desenvolverse en forma eficiente en dicho ámbito con la importancia de no abrumar al lector con detalles de difícil comprensión. En este libro, Moyano consigue alcanzar este complicado equilibrio. A lo largo de los distintos capítulos, el autor va repasando, en primera persona y con un lenguaje llano, simple y accesible, las principales modalidades de ciberdelito previstas en el Código Penal, e incluso aquellas conductas dañinas que todavía no han sido penalizadas por el legislador nacional, como la "porno venganza". También, y sobre todo, las estrategias y "buenas prácticas" vinculadas a la investigación de estos delitos (incluyendo el desarrollo de una "teoría del caso" y los pasos para definirla, la relación con organismos internacionales y empresas de tecnología y el cuidado de la "cadena de custodia" de la evidencia digital); así como las principales herramientas y fuentes de información disponibles (entre ellas, el sistema VAIC, la recopilación de información de fuente abierta —OSINT—, la que puede obtenerse de las compañías telefónicas, etcétera).

A lo largo de esta obra, además de evidenciar un acabado conocimiento sobre la materia que es objeto de análisis, Moyano demuestra gran capacidad para transmitirlo al lector, que recibe la información como si se la estuviese contando un amigo. Asimismo, afincado en su experiencia como fiscal especializado en la provincia de Buenos Aires, se muestra como un investigador moderno, que no se ciñe únicamente a los aspectos técnicos, sino que se preocupa, además, por resaltar la necesidad de mostrar empatía hacia las víctimas de estos nuevos delitos y aproximarse al análisis de los hechos con perspectiva de género.

La relación entre las nuevas tecnologías y la prevención, persecución y juzgamiento de delitos es una temática de enorme amplitud, en constante evolución a partir del surgimiento de nuevas modalidades delictivas, problemáticas, estrategias de investigación y herramientas tecnológicas. Se trata, también, de una materia que

puede ser abordada de muchas maneras distintas y con diferentes enfoques, con una aproximación más academicista o una más orientada a la práctica, como es el caso del libro que me toca prologar. En tal contexto, no cabe más que celebrar la aparición de una nueva voz, de un nuevo autor que demuestra, en este trabajo, que tiene mucho para aportar.

HERNÁN BLANCO

BUENOS AIRES, 13 DE MARZO DE 2024