LA CIBERCRIMINALIDAD

Consideración Criminológica, Político-Criminal, Dogmática, Procesal y Cooperación Internacional

2da Edición

COLECCIÓN CIENCIAS JURÍDICAS

COLECCIÓN CIENCIAS JURÍDICAS
Serie Derecho y gobernanza de lo público

LA CIBERCRIMINALIDAD

CONSIDERACIÓN CRIMINOLÓGICA, POLÍTICO-CRIMINAL, DOGMÁTICA, PROCESAL Y COOPERACIÓN INTERNACIONAL

2da Edición

BONIFACIO MENESES GONZÁLES

JEAN PAUL MENESES OCHOA

Prologo para la Segunda Edición Sr. Dr. Manuel Lázaro Pulido
Doctor en filosofía y letras (PhD), por la Universidad Pontificia de Salamanca
Del Reino de España.

Prefacio por Sr. Dr. Antoni Bosch Pujol
Director General (CEO): Institute of Audit & IT-Governance (IAITG). Data Privacy Institute (DPI) dentro del ISMS Forum. Docente de Pacífico Business School, Centrum-PUCP (Perú) y Universidades en España

Presentación Sr. Dr. Néstor Raúl Posada Arboleda
Rector de la Universidad de Medellín - Colombia.

UPSA EDICIONES

UNIVERSIDAD PONTIFICIA DE SALAMANCA

SALAMANCA
2026

Esta Editorial es miembro de la Unión de Editoriales Universitarias Españolas (UNE), lo que garantiza la difusión y comercialización nacional e internacional de sus publicaciones.

Universidad Pontificia de Salamanca
Compañía, 5 • Teléf. 923 27 71 28

publicaciones@upsa.es • www.publicaciones.upsa.es

Imagen portada: Depositphotos

I.S.B.N.:
Depósito Legal:

ÍNDICE GENERAL

GLOSARIO[1]

- **Adware:** Tipo de software malicioso cuya instalación hace que la computadora muestre o descargue publicidad de manera automática.
- **Applet:** Programas desarrollados con Java para mejorar la presentación de las páginas Web que realizan animaciones, juegos e interacción con el usuario.
- **Archivo:** Documento generado con una aplicación que se almacena en una unidad.
- **Backbone:** La columna vertebral de la Red.
- **Bomba lógica:** Clase de virus que carece de la capacidad de replicación y que consiste en una cadena de código que se ejecuta cuando una determinada condición se produce, por ejemplo, tras encender el ordenador una serie de veces, o pasados una serie de días desde el momento en que la bomba lógica se instaló en nuestro ordenador.
- **Bookmark:** Marca, anotación de una dirección Web o URL que queda archivada para su posterior uso.
- **Buscador:** Servidor de Internet que organiza los ficheros por grupos temáticos y que permite la localización de páginas Web mediante unas palabras clave que introduce el usuario, sin necesidad de conocer las direcciones de las citadas páginas.
- **Caballo de Troya (troyano):** Programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa.
- **Carding:** Es un término que describe el tráfico y el uso no autorizado de tarjetas de crédito. Las tarjetas de crédito robadas o los números de tarjetas de crédito se utilizan luego para comprar tarjetas de regalo prepagas para encubrir las huellas.
- **Ciberespacio:** Espacio virtual, no geográfico, determinado por la interconexión de personas a través de redes telemáticas.
- **Ciberpunk:** El ciberpunk es un subgénero de la ciencia ficción, conocido por reflejar visiones distópicas del futuro en las cuales se combinan la tecnología avanzada con un bajo nivel de vida.

[1] Las definiciones fueron obtenidas de diversas fuentes las cuales se señalan en la presente obra.

- **Cloacker:** Es un término inglés para denominar ciertas técnicas de posicionamiento web con el fin de engañar a los motores de búsqueda y mejorar la posición en los resultados.
- **Cookies:** Mecanismos que permiten a los gestores de cada página web grabar las entradas y salidas de los usuarios que acceden a su servidor. Es como si dejáramos nuestra tarjeta de visita
- **Cracker:** El desarrollo de esta actividad implica que se está cometiendo un acto delictivo, violándose la intimidad del afectado, la confidencialidad de la información y, específicamente en el caso del cracking, por el hecho de haber causado daños, cambios y/o destrucción de información, así como por haber inhabilitado soportes físicos como puedan ser: servidores, discos duros, etc.
- **Crash program:** Es la condición en la cual una aplicación informática, ya sea un programa o parte o la totalidad del sistema operativo dejan de funcionar de la forma esperada y dejan de responder a otras partes del sistema. A veces el programa simplemente aparece como "congelado", esto es: no responde a ninguna acción del usuario o del entorno operativo. Si el programa que falla es una parte crítica del núcleo del sistema operativo, el equipo completo puede dejar de responder (*crash de sistema).*
- **Criptografía:** Disciplina matemática e informática relacionada con la seguridad de la información, particularmente con el cifrado y la autenticación. En cuanto a la seguridad de aplicaciones y redes, es una herramienta para el control de acceso, la confidencialidad de la información y la integridad.
- **Data diddling:** El traspaso de datos es un tipo de delito cibernético en el que los datos se modifican a medida que se ingresan en un sistema informático, con mayor frecuencia por un empleado de entrada de datos o un virus informático. El procesamiento computarizado de los datos alterados da como resultado un beneficio fraudulento.
- **Dirección IP:** Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/ conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.
- **Dirección URL:** Es el mecanismo usado por los navegadores para obtener cualquier recurso publicado en la web. URL significa Uniform Resource Locator (Localizador de Recursos Uniforme). Una URL no es más que una dirección que es dada a un recurso único en la Web.

- **Disco duro:** (En inglés Hard Disk Drive, HDD) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales.
- **E-mail:** Nombre inglés que designa el correo electrónico.
- **Esteganografía:** La esteganografía trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, para que no se perciba su existencia.
- **Exploit:** Es una palabra inglesa que significa *explotar* o *aprovechar*, y que en el ámbito de la informática es un fragmento de *software*, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.
- **Firewall:** Dispositivos de seguridad a entradas no autorizadas.
- **Firma digital:** Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- **Freeware:** De libre distribución para el usuario y no utilizable con fines comerciales.
- **Gigabyte:** Unidad de medida de una memoria. 1 gigabyte = 1024 megabytes = 1.073.741.824 bytes.
- **Gusano:** Programa que está diseñado para copiarse y propagarse por sí mismo mediante mecanismos de red. No realizan infecciones a otros programas o ficheros.
- **Hacker:** Persona que a través de medios técnicos o de ingeniería social consigue acceder o introducirse en un sistema informático con intenciones diversas. Ya sea por simple entretenimiento o con la intención de descifrar el funcionamiento interno de los equipos y servidores de Internet asaltando así, los sistemas de seguridad sin ocasionar daños en ellos.
- **Hacking tool:** Las Hacktools (herramientas de hacking) se utilizan para habilitar nuevos usuarios en la lista de visitantes permitidos en el sistema, así como para borrar la información de los registros del sistema con el fin de ocultar la presencia de un usuario malicioso en éste.
- **Hardware:** Soporte físico del sistema computacional., todo lo tangible del computador, corresponde al Hardware.
- **Header:** Cabecera (header en inglés) se refiere a la información suplementaria situada al principio de un bloque de información que va a ser almacenada o transmitida y que

contiene información necesaria para el correcto tratamiento del bloque de información.

- Hijacker: Se trata de un tipo de ataque informático en el que los Hijackers son capaces de modificar la redirección de los servidores DNS. Significa que cuando un usuario quiera entrar a un dominio determinado, el DNS le devuelve una dirección de IP diferente.
- Home Page: Página primaria o introductoria a Internet. También llamada página de inicio.
- Internet: Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.
- Java: Lenguaje de programación creado por Sun Microsystem para proporcionar más velocidad y facilidad de uso a Internet, es independiente de la plataforma utilizada y está disponible para cualquier navegador de la WWW que admita este lenguaje.
- Javascript: Es un lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico.
- Joke: Son programas que a diferencia de los virus no tienen efectos destructivos y simulan realizar acciones en el ordenador como si de un virus se tratase. Son bromas, en ocasiones de mal gusto, que pueden generar confusión entre los usuarios y que por tanto pueden causar perjuicios.
- Mailbomb: El e-mail bombing es una técnica que utilizan los piratas informáticos para saturar una dirección, para intentar colar malware o simplemente para lograr que abramos un enlace o nos registremos en un servicio. En ocasiones está muy relacionado con el Spam o correo basura.
- Malware: (En inglés Malicius Software) Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.
- Memoria: También llamada almacenamiento, se refiere a parte de los componentes que forman parte de una computadora. Son dispositivos que retienen datos informáticos durante algún intervalo de tiempo.

- **Overclocking:** Operación consistente en forzar al procesador a trabajar a una velocidad superior a la original.
- **Password:** Clave secreta personal.
- **Phising:** Método de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño o la picaresca, recurriendo a la suplantación de la identidad digital de una entidad de confianza en el ciberespacio.
- **Placa base:** La placa base es esa en la que se conectan todos los componentes internos del ordenador, desde el procesador hasta los discos duros, la memoria RAM o la tarjeta gráfica. Cada uno de estos componentes tiene su propia ranura para que puedas conectarla.
- **Procesador:** Una unidad central de procesamiento, o CPU, es una pieza de hardware que permite que tu computadora interactúe con todas las aplicaciones y programas instalados. Una CPU interpreta las instrucciones del programa y crea la señal de pantalla con la que interactúas cuando utilizas una computadora.
- **Scanning:** Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos.
- **Scripkiddie:** Es un término utilizado de forma despectiva para describir a aquellos que utilizan programas y scripts desarrollados por otros expertos para atacar sistemas de computadoras y redes.
- **Shareware:** Se denomina shareware a una modalidad de distribución de software, en la que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso.
- **Sistema operativo:** Un sistema operativo es el conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software. Estos programas se ejecutan en modo privilegiado respecto de los restantes.
- **Skinning:** El skimming se deriva del verbo en inglés "to skim" (leer con rapidez) y se trata de un fraude que se hace a las tarjetas de crédito y débito. Esta estafa consiste en acceder a los datos de tu medio de pago a través de su banda magnética, mediante el uso tecnologías especiales. Existen diferentes medios para hacer skimming, pero los más comunes se dan

en cajeros automáticos y puntos de venta, mediante la instalación de un micro dispositivo llamado skimmer, que captura y transfiere de manera automática la información de tu tarjeta a los delincuentes.

- **Software:** Término general que designa los diversos tipos de programas usados en computación.
- **Spam:** Correo electrónico no solicitado. Se lo considera poco ético, ya que el receptor paga por estar conectado a Internet.
- **Spoofing:** La suplantación de identidad o spoofing en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
- **Spyware:** El programa espía es un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.
- **Superzapping:** Uso no autorizado de programas especiales (superzapping). Hace referencia a la utilización no autorizada de cualquier programa para alterar datos y resultados, u obtener información.
- **Virus informático:** Programa que está diseñado para copiarse a sí mismo con la intención de infectar otros programas o ficheros.
- **Warez:** Programas pirateados.

FUENTES DEL GLOSARIO

Adware:	https://latam.kaspersky.com/resource-center/threats/types-of-malware
Applet:	https://clasew.jimdofree.com/conceptos-b%C3%A1sicos-de-una-pagina-web/
Archivo:	https://acortar.link/kakLV3
Backbone:	https://acortar.link/q8MhCf
Bomba lógica:	http://www.dit.upm.es/~pepe/401/2150.htm#!-alone
Bookmark:	https://www.lawebdelprogramador.com/diccionario/Bookmark/
Buscador:	https://acortar.link/ECz6Hz
Caballo de troya (troyano):	https://proyectoa.com/glossary/caballo-de-troya/
Carding:	https://acortar.link/rhC9Jc
Ciberespacio:	https://www.um.es/docencia/barzana/IAGP/IAGP2-Internet-introduccion.html
Ciberpunk:	https://es.wikipedia.org/wiki/Ciberpunk
Cloacker:	https://acortar.link/mDHnbq
Cookies:	https://acortar.link/IUeqBv
Cracker:	https://proyectoa.com/glossary/cracker/
Crash Program:	https://es.wikipedia.org/wiki/Crash_(inform%C3%A1tica)#:~:text=En%20inform%C3%A1tica%2C%20un%20crash%20es,a%20otras%20partes%20del%20sistema
Criptografía:	http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012#:~:text=La%20Criptograf%C3%ADa%20es%20una%20disciplina,las%20herramientas%20id%C3%B3neas%20para%20ello
Data diddling:	https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Dirección IP:	https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP#:~:text=Una%20direcci%C3%B3n%20IP%20(del%20ingl%C3%A9s,red%20del%20modelo%20TCP%2FIP
Dirección URL:	https://developer.mozilla.org/es/docs/Learn/Common_questions/Web_mechanics/What_is_a_URL
Disco duro:	https://es.wikipedia.org/wiki/Unidad_de_disco_duro
E-mail:	https://www.ingles.com/comparar/email/username
Esteganografía:	https://latam.kaspersky.com/resource-center/definitions/what-is-steganography
Exploit:	https://www.uaesp.gov.co/sig/documentos/gestionti/editables/GTI-PC-17%20V1%20Pruebas%20de%20penetracion%20en%20entornos%20controlados.pdf
Firewall:	https://blog.invgate.com/es/deteccion-de-dispositivos-no-autorizados
Firma digital:	https://firmaelectronica.gob.es/Home/Empresas/Base-Legal.html#:~:text=3.1)%20La%20firma%20electr%C3%B3nica%20es,medio%20de%20identificaci%C3%B3n%20del%20firmante.
Freeware:	https://es.wikipedia.org/wiki/GNU_General_Public_License
Gigabyte:	https://www.xataka.com/basics/megabyte-gigabyte-terabyte-petabyte-cuales-son-las-diferencias
Gusano:	https://www.idearius.com/es/blog/tipos-de-malware-virus-troyano-spyware-gusano/#:~:text=Gusano%20inform%C3%A1tico%3A%20programa%20que%20se,no%20necesita%20alterar%20otros%20archivos.
Hacker:	https://www.dit.upm.es/~pepe/401/index.html#!4647
Hacking tool:	https://encyclopedia.kaspersky.es/knowledge/hacktool/
Hardware:	https://es.wikipedia.org/wiki/Hardware#:~:text=El%20hardware%20(pronunciado%20%5Bxard.,componentes%20el%C3%A9ctricos%2C%20electr%C3%B3nicos%20y%20electromec%C3%A1nicos.
Header:	https://es.wikipedia.org/wiki/Cabecera_(inform%C3%A1tica)

Hijacker:	https://www.optimaweb.es/hijacking-que-es-y-como-prevenir-ataques/#:~:text=Podemos%20decir%20que%20el%20secuestro,%2C%20a%20otra%20p%C3%A1gina%20web
Home page:	https://www.atinternet.com/es/glosario/landing-page/
Internet:	https://www.mendoza.gov.ar/dic/internet/#:~:text=Es%20un%20conjunto%20descentralizado%20de,l%C3%B3gica%20%C3%BAnica%2C%20de%20alcance%20mundial.
Java:	https://multimedia.uned.ac.cr/pem/internet_llega_al_aula/InternetAula/diseno/java.htm#:~:text=Java%20es%20un%20lenguaje%20de,hipertexto%20como%20el%20lenguaje%20html.
Javascript:	https://www.velneo.com/blog/que-es-javascript#:~:text=JavaScript%20es%20un%20lenguaje%20de,en%20la%20interfaz%20de%20usuario.
Joke:	https://www.pandasecurity.com/es/support/card?Id=10110#:~:text=Los%20Jokes%20son%20programas%20que,por%20tanto%20pueden%20causar%20perjuicios.
Mailbomb:	https://zonavirus.com/noticias/2021/e-mail-bombing-como-usan-el-spam-para-atacar_71650
Malware:	https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera#:~:text=La%20palabra%20malware%20viene%20del,el%20consentimiento%20de%20su%20propietario
Memoria:	https://es.wikipedia.org/wiki/Memoria_(inform%C3%A1tica)
Overclocking:	https://www.xataka.com/basics/overclock-que-que-ventajas-ofrece-que-desventajas-puede-tener
Password:	https://phoenixnap.mx/glosario/llave-secreta#:~:text=Glosario%20%C2%BB%20S%20%C2%BB%20%C2%BFQu%C3%A9%20es,en%20cifrado%20sim%C3%A9trico%20y%20asim%C3%A9trico.
Phishing:	https://www.ucv.edu.pe/blog/proteja-su-informacion-confidencial-como-identificar-y-evitar-el-phishing-una-tecnica-utilizada-por-estafadores/#:~:text=El%20phishing%20es%20una%20t%C3%A9cnica,obtener%20informaci%C3%B3n%20personal%20y%20confidencial.

Placa base:	https://www.xataka.com/basics/partes-placa-base-te-explicamos-sus-componentes-forma-sencilla-entiendas-que-tiene
Procesador:	https://www.hp.com/mx-es/shop/tech-takes/que-es-la-velocidad-del-procesador-y-por-que-es-importante
Scanning:	https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/
Skripkiddie:	http://www.redjaen.es/francis/?m=c&o=174713#:~:text=Script%20kiddie%20o%20Skiddie%20%2D%20Parecido,sistemas%20de%20computadoras%20y%20redes.
Shareware:	https://es.wikipedia.org/wiki/Shareware
Sistema operative:	https://es.wikipedia.org/wiki/Sistema_operativo
Skimming:	https://www.pichincha.com/portal/blog/post/que-es-el-skimming
Software:	https://www.eafit.edu.co/servicios-en-linea/cinf/Documents/glosario-informatico.pdf
Spam:	https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-stop-spam-texts
Spoofing:	https://www.foc.es/2018/10/19/4699-ciberseguridad-que-es-el-spoofing.html
Spyware:	https://www.ciset.es/glosario/488-spyware#:~:text=El%20Spyware%2C%20tambi%C3%A9n%20denominado%20spybot,permiso%20del%20due%C3%B1o%20del%20ordenador.
Superzapping:	https://www.scenacriminis.com/ciencias-forenses/tipologia-del-fraude-informatico/
Virus informático:	https://www.idearius.com/es/blog/tipos-de-malware-virus-troyano-spyware-gusano/#:~:text=Virus%3A%20malware%20que%20se%20copia,ag%C3%A1rrenme%20si%20pueden!%C2%BB)
Warez:	https://es.wikipedia.org/wiki/Warez

PROLOGO SEGUNDA EDICION

Escribir un prólogo es un ejercicio que combina responsabilidad intelectual y cercanía personal. No se trata simplemente de introducir una obra, sino de situarla en su contexto académico, reconocer su alcance y ofrecer al lector una clave de interpretación. Cuando, además, el libro que se presenta es fruto de la amistad, del respeto profesional y del diálogo sostenido a lo largo del tiempo, la tarea adquiere una dimensión añadida: la de dar testimonio.

Conozco al **doctor Bonifacio Meneses Gonzales**, nuestra relación nació en el marco del Instituto Iberoamericano de Justicia y cuando en la época era director del Servicio de Publicaciones de la Universidad Pontificia de Salamanca (UPSA Ediciones), pero pronto trascendió lo estrictamente profesional para convertirse en una amistad fundada en el aprecio intelectual y humano. A lo largo de ese tiempo he podido constatar su compromiso con el estudio serio del derecho penal, su vocación institucional y su permanente inquietud por comprender los desafíos contemporáneos que afectan a la administración de justicia. Ese mismo compromiso se advierte en la trayectoria de **Jean Paul Meneses Ochoa**, cuya formación académica rigurosa y sensibilidad jurídica actualizan, con mirada propia, el legado recibido.

La colaboración entre padre e hijo que cristaliza en esta obra no es un dato anecdótico. Representa, en el ámbito jurídico, algo profundamente significativo: la transmisión intergeneracional del saber cómo continuidad creativa. No se trata de repetir lo aprendido, sino de dialogar con él, ampliarlo y proyectarlo hacia nuevos horizontes. Esta segunda edición confirma que esa colaboración no fue circunstancial, sino la expresión de una vocación compartida por comprender y ordenar jurídicamente uno de los fenómenos más complejos de nuestro tiempo: la cibercriminalidad.

La primera edición de este tratado ya se distinguió por su ambición sistemática. No era un manual introductorio ni una recopilación de comentarios legislativos. Era —y sigue siendo— un intento serio de ofrecer una visión integral del fenómeno, articulando perspectivas criminológicas, político-criminales, dogmáticas, procesales y de cooperación internacional. Esta segunda edición no se limita a actualizar datos; profundiza y consolida un método.

El lector advertirá, desde las primeras páginas, que el punto de partida no es meramente técnico. La obra comienza con una reflexión amplia sobre la informática, Internet, la sociedad de la información y el ciberespacio como

nuevo ámbito de interacción humana. Este planteamiento inicial es decisivo. El delito no puede entenderse sin comprender el entorno en el que surge. La cibercriminalidad no es simplemente la comisión de ilícitos mediante ordenadores; es un fenómeno que nace en una transformación estructural de la vida social.

El ciberespacio no es un simple soporte técnico, sino un entorno relacional con características estructurales propias que transforman las dinámicas sociales y, con ellas, la configuración jurídica de los conflictos. Su arquitectura descentralizada, sin un centro único de control, diluye las fronteras entre lo público y lo privado y complica la determinación de la competencia jurisdiccional y de las responsabilidades. A ello se suma el anonimato relativo, que aunque no es absoluto, favorece conductas desinhibidas y dificulta la identificación del autor, generando además en la víctima una sensación persistente de indefensión. La deslocalización geográfica cuestiona los criterios clásicos de territorialidad, pues una acción realizada en un país puede producir efectos inmediatos y simultáneos en varios Estados, amplificando el alcance del daño.

Estas notas estructurales se completan con la instantaneidad comunicativa, la capacidad de almacenamiento masivo de datos y la replicabilidad ilimitada de contenidos. La velocidad y viralidad de la red intensifican la lesión y dificultan su contención; la permanencia de la información convierte el daño en duradero; y la posibilidad de copia infinita transforma agresiones tradicionalmente acotadas —como la injuria o la difamación— en afectaciones globales y persistentes. Así, el ciberespacio no solo facilita nuevas formas de ataque a bienes jurídicos clásicos, sino que altera cualitativamente la naturaleza del perjuicio, obligando al derecho penal a reinterpretar categorías como publicidad, permanencia y difusión masiva para responder adecuadamente a una realidad estructuralmente distinta.

Por ello, la obra acierta al dedicar un análisis detenido a los caracteres intrínsecos y extrínsecos del ciberespacio, pues solo desde esa comprensión estructural es posible elaborar una respuesta jurídico-penal coherente. La transaccionalidad del entorno digital —esto es, su configuración como espacio de intercambio constante de datos, servicios y contenidos— convierte cada interacción en potencialmente relevante desde el punto de vista jurídico. No se trata únicamente de actos aislados, sino de flujos continuos de información que pueden ser interceptados, alterados o instrumentalizados. La universalidad del ciberespacio, por su parte, elimina las barreras tradicionales de acceso y multiplica exponencialmente el alcance de cualquier conducta, ampliando el círculo de posibles víctimas. La anonimatización, ya sea real o percibida, favorece

dinámicas de desinhibición y fragmenta la trazabilidad de la acción, mientras que la mutabilidad tecnológica introduce un factor de inestabilidad permanente: las herramientas cambian con rapidez, surgen nuevas plataformas, se modifican protocolos y aparecen formas inéditas de interacción.

Comprender estos rasgos no es un ejercicio meramente descriptivo; implica reconocer que el fenómeno delictivo en el entorno digital no puede analizarse como una simple traslación instrumental de categorías tradicionales. El ciberespacio reconfigura la acción —que puede ser automatizada, distribuida o ejecutada a distancia—, la autoría —que puede diluirse en redes colaborativas, bots o estructuras descentralizadas— y la victimización —que puede adquirir carácter masivo, simultáneo o prolongado en el tiempo—. La obra pone de relieve que el injusto penal se ve afectado no solo en su modalidad comisiva, sino en su intensidad y proyección, obligando a repensar criterios como dominio del hecho, participación, tentativa o consumación en contextos digitales complejos.

Desde el punto de vista criminológico, el tratado ofrece además un estudio riguroso y sistemático del perfil del ciberdelincuente y de la ciber víctima. Se distingue entre el delincuente especializado —con conocimientos técnicos avanzados y capacidad de planificación sofisticada— y el actor oportunista o aficionado, que aprovecha herramientas disponibles en la red sin comprender plenamente su funcionamiento. Esta tipología permite advertir que la cibercriminalidad no es homogénea: conviven estructuras organizadas, delincuencia económica transnacional y conductas individuales de acoso o fraude. Del mismo modo, el análisis de la ciber víctima subraya la existencia de factores de vulnerabilidad específicos, como la exposición constante en redes sociales, la falta de alfabetización digital o la confianza excesiva en entornos virtuales aparentemente seguros.

El estudio incorpora, con acierto, los factores facilitadores del delito en el ciberespacio: la conectividad permanente que elimina la separación entre tiempo laboral y tiempo personal; la sofisticación tecnológica que reduce costes de ejecución y aumenta la rentabilidad del delito; y la insuficiencia o fragmentación normativa que genera zonas grises aprovechables por los infractores. Especial importancia reviste el tratamiento de la "cifra negra" de la cibercriminalidad. La baja tasa de denuncia, motivada por desconocimiento, vergüenza o percepción de ineficacia institucional, junto con la dificultad de identificación de los autores, provoca una infrarrepresentación estadística del fenómeno. Al abordar esta dimensión oculta, la obra supera visiones simplistas que reducen el problema a

una cuestión meramente técnica y lo sitúa en el marco más amplio de la política criminal y la confianza institucional.

Particularmente relevante es el análisis dedicado a la inteligencia artificial, cuya incorporación en esta segunda edición resulta no solo pertinente, sino necesaria. La inteligencia artificial puede operar como herramienta de comisión delictiva —a través de deepfakes, suplantaciones de identidad, generación automatizada de contenidos engañosos o fraudes financieros asistidos por algoritmos—, pero también introduce desafíos conceptuales de mayor calado. ¿En qué medida puede hablarse de autoría cuando intervienen sistemas autónomos? ¿Cómo se determina la previsibilidad del resultado cuando el comportamiento del sistema es parcialmente autoaprendente? ¿Qué grado de control humano es exigible para fundamentar responsabilidad penal? La obra aborda estas cuestiones con equilibrio, evitando tanto el alarmismo tecnológico que propugna respuestas punitivas desproporcionadas como la trivialización que minimizaría su impacto real. Se opta, más bien, por una reflexión prudente, consciente de que la tecnología no sustituye la responsabilidad humana, pero sí exige una actualización rigurosa de los marcos dogmáticos tradicionales.

Desde la perspectiva dogmática, uno de los aportes más valiosos del libro es la delimitación conceptual de la cibercriminalidad. La distinción entre delitos cometidos a través de la informática y delitos cometidos contra la informática permite ordenar el análisis. En el primer caso, el medio tecnológico actúa como instrumento; en el segundo, el sistema informático o los datos constituyen el objeto directo de protección. Esta diferenciación, lejos de ser meramente terminológica, tiene consecuencias relevantes en la configuración típica y en la determinación del bien jurídico protegido.

El estudio del bien jurídico tutelado en la cibercriminalidad constituye otro de los núcleos centrales del tratado. La seguridad informática, la integridad y disponibilidad de los datos, la intimidad informativa y el correcto funcionamiento de los sistemas aparecen como bienes merecedores de protección penal específica. Aquí se advierte una evolución en la teoría del bien jurídico: junto a los bienes clásicos, emergen dimensiones nuevas vinculadas a la autodeterminación informativa y al entorno digital de la persona.

Esta evolución se relaciona con la emergencia de los llamados derechos de cuarta generación. El derecho al entorno virtual, a la protección de datos personales y a la identidad digital son manifestaciones de esa transformación. El registro de un dispositivo móvil no puede equipararse sin más al registro de un objeto físico tradicional. El volumen y la naturaleza de la información

almacenada exigen cautelas reforzadas. La obra subraya esta necesidad de adaptación normativa sin perder de vista las garantías fundamentales.

En el ámbito de la legislación nacional peruana, el análisis detallado de la Ley N.º 30096 y sus modificaciones constituye una herramienta de gran utilidad para operadores jurídicos. El examen pormenorizado de cada tipo penal —acceso ilícito, atentados contra la integridad de datos y sistemas, fraude informático, suplantación de identidad, chantaje sexual digital— revela un trabajo minucioso que combina exégesis normativa y reflexión crítica. No se trata de una simple descripción; se valoran aciertos y deficiencias, se identifican lagunas y se proponen mejoras.

Particularmente destacable es la atención prestada a la responsabilidad penal de las personas jurídicas en el ámbito de los ciberdelitos. En un contexto donde empresas tecnológicas, proveedores de servicios y plataformas digitales desempeñan un papel central, la delimitación de su eventual responsabilidad adquiere relevancia práctica y teórica. La obra aborda este tema con equilibrio, consciente de la necesidad de evitar tanto la impunidad estructural como la imputación indiscriminada.

La dimensión procesal ocupa un espacio significativo. La prueba electrónica plantea desafíos inéditos en cuanto a recolección, preservación, cadena de custodia y valoración judicial. La volatilidad de los datos, su fácil alteración y la necesidad de cooperación internacional exigen protocolos técnicos específicos. El tratado dedica un análisis exhaustivo a estas cuestiones, integrando estándares internacionales y experiencias comparadas. En este punto, la obra resulta especialmente útil para jueces, fiscales y peritos.

No menos relevante es el estudio de los procedimientos especiales —proceso inmediato y acusación directa— aplicables a los delitos informáticos. En contextos de alta incidencia delictiva, la eficacia procesal se convierte en componente esencial de la política criminal. Sin embargo, esa eficacia no puede alcanzarse a costa de las garantías. El equilibrio entre celeridad y respeto a los derechos fundamentales constituye una de las tensiones permanentes del derecho procesal penal contemporáneo.

La cooperación internacional ocupa un capítulo de singular importancia. La cibercriminalidad es, por definición, transnacional. Los criterios clásicos de territorialidad resultan insuficientes cuando la conducta se ejecuta en un país, los servidores se encuentran en otro y los efectos se producen en un tercero. El análisis del Convenio de Budapest y de sus protocolos adicionales, así como de

los mecanismos de cooperación regional, demuestra la conciencia de que ningún Estado puede afrontar aisladamente este fenómeno.

El estudio de los criptoactivos y las criptomonedas añade otra dimensión contemporánea. La utilización de estos instrumentos financieros en esquemas fraudulentos, blanqueo de capitales o evasión de controles regulatorios exige respuestas normativas sofisticadas. La obra analiza casos judicializados y debates doctrinales, contribuyendo a un campo todavía en evolución.

Finalmente, el tratamiento del ciberterrorismo y el ciberodio evidencia la complejidad del fenómeno cuando se entrecruzan libertad de expresión, seguridad pública y prevención de la radicalización. La red puede convertirse en plataforma de propaganda extremista o de incitación al odio. La respuesta penal debe ser cuidadosa para no erosionar indebidamente derechos fundamentales. La obra aborda esta cuestión con prudencia y sentido de proporcionalidad.

El contenido del libro despierta en mi espíritu una reflexión filosófica y es que el análisis dogmático de la cibercriminalidad no puede reducirse a una cuestión de técnica legislativa ni a un mero problema de actualización normativa. Lo que está en juego es, en último término, la comprensión de la persona humana en el entorno digital y la misión del derecho en la protección de su dignidad. La distinción entre delitos cometidos a través de la informática y delitos cometidos contra la informática no es solo una clasificación funcional; expresa una diferencia antropológica relevante: en un caso, la tecnología es instrumento al servicio de la acción humana; en el otro, el propio sistema digital y los datos se convierten en objeto de tutela porque en ellos se proyecta la vida personal y social de los individuos. La técnica deja de ser neutral cuando se convierte en espacio de realización o vulneración de la persona.

La tradición de la democracia cristiana —arraigada en la centralidad de la dignidad humana, el personalismo comunitario y el principio del bien común— ofrece un marco especialmente fecundo para interpretar esta evolución. Si la persona es el fundamento y fin del orden jurídico, como ha sostenido de manera constante la doctrina social cristiana, entonces el entorno digital debe ser comprendido como una dimensión más de su existencia relacional. La seguridad informática, la integridad y disponibilidad de los datos, la intimidad informativa y el correcto funcionamiento de los sistemas no son meros bienes técnicos: son condiciones estructurales para el ejercicio de la libertad, la participación y la responsabilidad en la sociedad contemporánea.

La ampliación del catálogo de bienes jurídicos hacia la autodeterminación informativa y la identidad digital puede leerse, desde esta perspectiva, como una

actualización del principio personalista. El ser humano no se agota en su corporeidad ni en su presencia física; su identidad se proyecta hoy en redes, perfiles, bases de datos y sistemas interconectados. Proteger el entorno digital no significa absolutizar la tecnología, sino salvaguardar la esfera de libertad en la que la persona desarrolla su vida social. La emergencia de los llamados derechos de cuarta generación —protección de datos, derecho al entorno virtual, identidad digital— no representa una ruptura con la tradición, sino una profundización de la misma: es la extensión del principio de dignidad a nuevas formas de vulnerabilidad.

En este sentido, la exigencia de cautelas reforzadas en el registro de dispositivos móviles o en el tratamiento de datos personales responde a una intuición profundamente coherente con el pensamiento cristiano: la persona no puede ser reducida a objeto de control ni a mera fuente de información. El volumen y la naturaleza de los datos almacenados en un dispositivo digital revelan aspectos íntimos de la vida, las relaciones y las convicciones del individuo. Una intervención estatal desproporcionada podría afectar no solo la privacidad, sino la libertad de conciencia y la autonomía moral. La democracia cristiana, que históricamente ha defendido el Estado de derecho y la limitación del poder, encuentra aquí un campo privilegiado para reafirmar el principio de proporcionalidad y el respeto a las garantías fundamentales.

El análisis de la legislación nacional —como en el caso de la Ley N.º 30096 y sus modificaciones— puede interpretarse también desde el prisma del bien común. El derecho penal no es un instrumento de reacción automática, sino una expresión de la responsabilidad pública en la protección de las condiciones básicas de convivencia. Tipos penales como el acceso ilícito, el fraude informático o la suplantación de identidad no solo tutelan intereses individuales, sino la confianza social en los sistemas digitales que sostienen la vida económica y administrativa. La democracia cristiana, que subraya la dimensión comunitaria de la persona, reconoce que la seguridad de los sistemas informáticos no es un fin en sí mismo, sino una garantía para la participación equitativa y justa en la vida social.

Particular relevancia adquiere, en este marco, la cuestión de la responsabilidad penal de las personas jurídicas. Las empresas tecnológicas, plataformas y proveedores de servicios ocupan hoy un lugar estructural en la configuración del espacio público digital. Desde una perspectiva personalista, no puede aceptarse una impunidad estructural que derive de la complejidad organizativa; pero tampoco sería compatible con el principio de justicia atribuir responsabilidad de forma indiscriminada, sin atender a la capacidad real de

control y prevención. La democracia cristiana ha defendido históricamente el principio de subsidiariedad: cada instancia social debe asumir la responsabilidad que le corresponde, sin que el Estado sustituya injustificadamente a la sociedad, pero tampoco renuncie a su función reguladora cuando el bien común está en riesgo. La delimitación equilibrada de la responsabilidad empresarial en el ámbito digital responde precisamente a esa lógica.

En el ámbito procesal, los desafíos de la prueba electrónica, la cadena de custodia digital y la cooperación internacional exigen una reflexión que no sacrifique garantías en nombre de la eficacia. La tensión entre celeridad y respeto a los derechos fundamentales es una constante del derecho penal contemporáneo. Desde la tradición democrática cristiana, la eficacia del sistema no puede convertirse en valor absoluto. La justicia no se mide únicamente por la rapidez de la respuesta, sino por su conformidad con la dignidad humana y el debido proceso. El proceso inmediato y la acusación directa pueden ser instrumentos legítimos de política criminal, pero solo en la medida en que se inserten en un marco de garantías sólidas y control judicial efectivo.

La dimensión transnacional de la cibercriminalidad plantea, asimismo, un desafío que interpela la concepción misma de soberanía. La cooperación internacional —reflejada en instrumentos como el Convenio de Budapest— expresa la necesidad de una solidaridad jurídica entre Estados frente a fenómenos que superan las fronteras. La democracia cristiana, con su vocación universalista y su énfasis en la fraternidad entre pueblos, encuentra aquí un terreno propicio para afirmar que el bien común ya no puede concebirse exclusivamente en clave nacional. La protección de la persona en el entorno digital requiere estructuras de colaboración que respeten las identidades jurídicas de cada Estado, pero que reconozcan la interdependencia global.

El estudio de los criptoactivos y las criptomonedas introduce otra dimensión ética relevante. La innovación financiera puede ser instrumento de inclusión y desarrollo, pero también vehículo de fraude y blanqueo. Desde la perspectiva de la justicia social, la regulación de estos instrumentos debe orientarse a evitar que la opacidad tecnológica se convierta en refugio de prácticas lesivas para la comunidad. La libertad económica, valor reconocido por la tradición cristiana, no es absoluta; está ordenada al bien común y subordinada al respeto de la dignidad humana.

Finalmente, el tratamiento del ciberterrorismo y del ciberodio confronta directamente la tensión entre libertad de expresión y protección de la convivencia democrática. La red puede ser espacio de deliberación pública y

participación ciudadana, pero también de radicalización y propagación del odio. La respuesta penal debe ser prudente y proporcionada, evitando tanto la tolerancia ingenua como la restricción excesiva. Desde la democracia cristiana, la libertad no se entiende como mera ausencia de límites, sino como libertad responsable, orientada a la verdad y al respeto del otro. La sanción del discurso que incita a la violencia o al odio encuentra fundamento en la defensa de la dignidad de las personas y de la paz social, pero exige una delimitación cuidadosa que no erosione la pluralidad democrática.

En síntesis, la reflexión dogmática sobre la cibercriminalidad, leída desde la filosofía del derecho en el ámbito de la democracia cristiana, revela que el desafío digital no es solo técnico, sino antropológico y político. La tarea del derecho consiste en integrar la innovación tecnológica en un orden jurídico que coloque a la persona en el centro, promueva el bien común y limite el poder —tanto público como privado— conforme a criterios de justicia y proporcionalidad. Solo así la sociedad digital podrá desarrollarse como espacio de libertad auténtica y no como escenario de nuevas formas de dominación o exclusión.

Más allá de la amplitud temática, lo que distingue a este tratado es su coherencia interna. Cada capítulo se integra en una arquitectura conceptual que permite comprender el fenómeno en su conjunto. No se trata de piezas aisladas, sino de un sistema ordenado. Esa sistematicidad es, a mi juicio, uno de los mayores méritos de la obra.

Vivimos en una época en la que la tecnología avanza a un ritmo que desafía la capacidad de adaptación normativa. Lo que hoy parece novedoso mañana puede resultar obsoleto. En este contexto, el derecho penal enfrenta un doble riesgo: reaccionar de forma precipitada o quedar rezagado. Entre ambos extremos se sitúa la prudencia reflexiva que este libro encarna. La reflexión precede a la norma; la comprensión precede a la sanción.

Concluiré regresando al punto inicial: la amistad intelectual. Este libro no es solo el resultado de investigación académica; es fruto de un diálogo sostenido, de una vocación compartida por comprender y servir. La colaboración entre padre e hijo simboliza esa continuidad que da profundidad al estudio. En tiempos marcados por la inmediatez, esta obra representa la perseverancia.

Estoy convencido de que esta segunda edición consolidará su posición como referencia obligada en el ámbito iberoamericano. Y también estoy persuadido de que no será la última. La materia evoluciona y exigirá nuevas revisiones. Pero contar con un fundamento sólido es imprescindible, y este tratado lo ofrece.

Con gratitud por la confianza depositada en mí y con sincera admiración por el trabajo realizado, entrego estas palabras al lector como invitación a una lectura atenta. Que este prólogo sirva de puente entre la experiencia académica que me une a los autores y la comunidad jurídica que encontrará en estas páginas un instrumento valioso para afrontar uno de los desafíos más significativos del derecho penal contemporáneo.

Manuel Lázaro Pulido

Doctor en Filosofía (PhD)
Universidad Pontificia de Salamanca
Universidad Internacional de La Rioja

PREFACIO SEGUNDA EDICION

Redactar el prefacio de una obra científica dedicada a la cibercriminalidad implica asumir una responsabilidad que trasciende la mera formalidad editorial. No se trata únicamente de introducir al lector en el contenido de un libro, sino de situarlo en el contexto intelectual, tecnológico y humano en el que la obra ha sido concebida.

La cibercriminalidad, lejos de constituir un fenómeno periférico del Derecho penal, se ha convertido en una manifestación estructural de la transformación digital de la sociedad, afectando la seguridad económica, la confianza institucional, la privacidad, la identidad y la propia percepción de vulnerabilidad de las personas en el entorno digital.

Aceptar la invitación de los doctores **Bonifacio Meneses Gonzáles** y **Jean Paul Meneses Ochoa** para redactar estas páginas constituye un honor académico que deseo agradecer expresamente. La confianza depositada no solo representa un reconocimiento intelectual, sino también un gesto de cercanía humana que valoro profundamente. La relación académica y personal construida a lo largo del tiempo, caracterizada por el intercambio de ideas, la coincidencia en inquietudes investigadoras y el compromiso compartido con la formación jurídica especializada, permite comprender con mayor claridad el esfuerzo, la dedicación y la vocación que sustentan esta obra.

La lectura del libro revela una intención que va más allá del análisis descriptivo del ciberdelito. Se percibe una voluntad de comprender el fenómeno en su complejidad, de integrar perspectivas y de ofrecer herramientas que permitan a juristas, investigadores, operadores judiciales y profesionales de la seguridad digital interpretar una realidad que evoluciona a un ritmo difícilmente comparable con otros ámbitos del conocimiento jurídico. Esa vocación integradora constituye, a mi juicio, uno de los principales valores del trabajo.

Mi aproximación personal al fenómeno digital se remonta a una etapa previa a la generalización de la informática. La formación como físico permitió comprender tempranamente que la tecnología no es únicamente un conjunto de herramientas, sino la materialización de modelos abstractos capaces de transformar la organización social. En ese contexto, los primeros contactos con la informática en la época de las tarjetas perforadas implicaban una relación particularmente rigurosa con la lógica del procesamiento de la información. La programación exigía anticipación, precisión y disciplina intelectual; cada

instrucción debía ser pensada con detenimiento y cada error obligaba a reconsiderar la estructura completa del proceso.

Aquella informática temprana generaba una conciencia profunda sobre la importancia de la arquitectura de los sistemas, sobre la fragilidad de los procesos y sobre la necesidad de comprender la lógica subyacente a la tecnología. Con el paso del tiempo, la evolución hacia la auditoría de sistemas de información permitió observar el entorno digital desde una perspectiva distinta: la del control, la seguridad y la confianza. La auditoría mostró que los sistemas informáticos no solo procesan datos, sino que constituyen infraestructuras críticas de confianza cuya vulneración puede producir consecuencias jurídicas, económicas y sociales de gran alcance.

Paralelamente, la progresiva especialización en protección de datos personales y en programas de cumplimiento normativo permitió constatar que la cibercriminalidad no puede analizarse de forma aislada de la gestión del riesgo organizacional. La privacidad, la seguridad de la información, la gobernanza de datos y los modelos de compliance constituyen hoy dimensiones interdependientes. La experiencia en proyectos de auditoría, implementación de sistemas de gestión y formación especializada en materia de protección de datos y compliance ha permitido observar que muchos incidentes de cibercriminalidad se originan precisamente en debilidades organizativas, culturales y de control que trascienden el ámbito puramente técnico.

Desde esta perspectiva, la obra adquiere un valor particularmente relevante para los oficiales de protección de datos personales y para los compliance officers. El ciberdelito no solo plantea retos penales, sino también obligaciones de prevención, gestión de incidentes, notificación de brechas, evaluación de impacto y diseño de controles técnicos, jurídicos y organizativos. La comprensión del fenómeno resulta esencial para quienes desempeñan funciones de supervisión, asesoramiento y control en organizaciones públicas y privadas. La obra ofrece, en este sentido, un marco conceptual que permite conectar la dimensión penal del ciberdelito con la gestión del riesgo, la responsabilidad corporativa y la cultura de cumplimiento.

Con el tiempo, la actividad académica vinculada a la protección de datos, la seguridad de la información, la gobernanza y el impacto de la inteligencia artificial ha reforzado la convicción de que el estudio del ciberdelito exige enfoques interdisciplinarios. La convergencia entre tecnología y Derecho no es una opción metodológica, sino una necesidad epistemológica. Las categorías jurídicas tradicionales se ven tensionadas por la desmaterialización de la

conducta, la automatización de los procesos, la multiplicidad de actores y la volatilidad de la evidencia digital.

En este sentido, la obra destaca por su capacidad de integrar la criminología, la política criminal, la dogmática penal, la dimensión procesal y la cooperación internacional en un marco coherente. La cibercriminalidad se presenta como un fenómeno técnico, jurídico y organizacional simultáneamente, lo que exige una lectura que reconozca la interacción entre arquitectura tecnológica, estructura normativa y sistemas de control corporativo.

Uno de los aspectos más relevantes del libro es la atención prestada a la evidencia digital. La prueba en el ámbito del ciberdelito exige comprender la naturaleza de los datos, su volatilidad, la necesidad de preservar la integridad de la información y la importancia de la cadena de custodia digital. La autenticidad y la trazabilidad de la evidencia no son meras cuestiones técnicas, sino elementos que determinan la eficacia del proceso penal y la protección de las garantías fundamentales. El tratamiento que la obra ofrece en este ámbito refleja una comprensión adecuada de la convergencia entre técnica, proceso y cumplimiento normativo.

Asimismo, la incorporación del análisis de tecnologías emergentes refuerza la actualidad del trabajo. La inteligencia artificial, los sistemas automatizados, los criptoactivos y las nuevas formas de interacción digital amplían el horizonte delictivo y generan desafíos regulatorios que requieren prudencia doctrinal, capacidad técnica y una adecuada cultura de cumplimiento dentro de las organizaciones.

El carácter transnacional del ciberdelito constituye otro de los ejes fundamentales del análisis. La arquitectura del ciberespacio desafía las nociones tradicionales de territorialidad y obliga a repensar la cooperación internacional, pero también la gobernanza corporativa y la responsabilidad organizacional en entornos digitales globalizados.

Desde la perspectiva académica y docente, la obra adquiere un valor particularmente significativo. La claridad expositiva, la amplitud temática y el equilibrio entre profundidad doctrinal y comprensión técnica la convierten en un texto idóneo para la formación de especialistas y para el desarrollo de investigaciones futuras. En coherencia con mi propia trayectoria investigadora y docente, este libro pasará a formar parte de la bibliografía de referencia en programas formativos relacionados con la protección de datos personales, el compliance, la seguridad de la información y el Derecho penal tecnológico, así

como en actividades de formación dirigidas a oficiales de protección de datos y responsables de cumplimiento.

Más allá de su densidad técnica y doctrinal, la obra mantiene una constante preocupación por la dimensión humana del fenómeno. La cibercriminalidad afecta personas, organizaciones y comunidades, recordándonos que la tecnología, pese a su complejidad, se inserta siempre en contextos humanos.

Al recordar los inicios en la informática de tarjetas perforadas resulta inevitable reflexionar sobre la extraordinaria evolución tecnológica que ha experimentado la sociedad. Aquella informática pausada, que exigía anticipación y respeto por la lógica de los sistemas, ha dado paso a un entorno digital ubicuo, automatizado e invisible en su complejidad. Sin embargo, la esencia permanece: la tecnología sigue siendo un sistema construido por personas, vulnerable a errores, manipulaciones y usos indebidos.

La cibercriminalidad es, en cierta medida, el reflejo inevitable de esa evolución. Allí donde existe innovación, aparecen nuevas formas de riesgo. Comprenderlas no implica únicamente desarrollar herramientas jurídicas, sino también asumir una responsabilidad académica, organizacional y social respecto al uso ético y seguro de la tecnología.

Agradezco profundamente a los autores la oportunidad de acompañar este proyecto y de compartir estas reflexiones desde la amistad académica que nos une. Confío en que la obra enriquecerá el debate doctrinal, estimulará nuevas investigaciones y se consolidará como texto de referencia para juristas, investigadores, oficiales de protección de datos y compliance officers que buscan comprender la complejidad del entorno digital sin perder de vista su dimensión humana.

Porque la tecnología evoluciona, los sistemas cambian y las amenazas se transforman, pero permanece constante la responsabilidad de comprender, enseñar y proteger. Ese es, en última instancia, el valor de esta obra y el motivo por el cual su lectura resulta no solo recomendable, sino necesaria

Antoni Bosch Pujol

Director General del Institute of Audit & IT-Governance (IAITG). Director de los cursos de Certificación en Protección de Datos e IA con la Pacífico Business School, y de Compliance Officer con Centrum-PUCP (Perú).

PRESENTACION SEGUNDA EDICION

La Universidad Pontificia de Salamanca y el Instituto Iberoamericano de Justicia asumen con alto compromiso académico, la responsabilidad editorial de la saga, Primera y Segunda edición de la obra ***Cibercriminalidad: Consideración criminológica, político-criminal, dogmática procesal y cooperación internacional***, texto que ofrece una visión integral y sistemática de uno de los fenómenos más complejos del derecho penal contemporáneo.

Desde el Reino de España, la Universidad Pontificia de Salamanca, institución de profunda tradición humanista y jurídica, reafirma su vocación de promover estudios que articulen ciencia, ética y compromiso social. A su vez, el Instituto Iberoamericano de Justicia fortalece, mediante esta publicación, el diálogo académico transnacional y la consolidación de estándares comunes en materia penal, procesal y de cooperación internacional dentro del espacio jurídico iberoamericano.

A este esfuerzo editorial se suma el aval institucional de la **Universidad de Medellín,** cuya trayectoria académica constituye un referente en la formación jurídica en América Latina. Fundada sobre sólidos principios humanistas, la Universidad de Medellín ha consolidado una escuela de pensamiento penal caracterizada por el rigor dogmático, la investigación aplicada y la apertura al diálogo comparado. Su Facultad de Derecho ha formado generaciones de juristas que hoy desempeñan funciones relevantes en la judicatura, el ministerio público, la academia y el ejercicio profesional en distintos países.

Entre las bondades que distinguen a esta Casa de Estudios se encuentran su permanente actualización curricular, la promoción de la investigación interdisciplinaria, la proyección internacional de sus programas de posgrado y el fomento de redes académicas con instituciones europeas y latinoamericanas. La Universidad no solo transmite conocimiento, sino que construye comunidad académica, impulsa la ética profesional y promueve el compromiso con el Estado social y democrático de derecho.

La obra aborda la cibercriminalidad desde cuatro dimensiones estructurales:

- Criminológica, examinando las dinámicas delictivas en entornos digitales, los nuevos perfiles criminógenos y los factores de riesgo asociados a la transformación tecnológica.
- Político-criminal, analizando las respuestas normativas del Estado, la proporcionalidad punitiva y el equilibrio entre seguridad y derechos fundamentales.

- Dogmática penal y procesal, desarrollando los problemas de tipicidad, autoría en estructuras descentralizadas, imputación objetiva, obtención y valoración de la prueba digital, así como las garantías constitucionales en la investigación tecnológica.

Cooperación internacional, destacando la necesidad de mecanismos eficaces de asistencia judicial, armonización normativa y estrategias multilaterales frente a delitos que trascienden fronteras.

Esta segunda edición ha sido enriquecida por el trabajo académico del doctor Jean Paul Meneses Ochoa, Magister en Derecho Penal por la Universidad de Medellín, así como por el profesor Bonifacio Meneses Gonzales, docente de la misma casa de estudios, quienes aportan una sólida perspectiva comparada y una rigurosa fundamentación dogmática.

Cabe destacar que la Universidad de Medellín, a través de su Rectorado, avala expresamente esta obra, reconociendo su valor científico, su actualidad y su contribución al fortalecimiento del pensamiento jurídico penal en el ámbito iberoamericano. Este respaldo institucional refleja la proyección internacional de su comunidad académica y la consolidación de una escuela jurídica comprometida con los desafíos de la era digital.

La articulación entre instituciones académicas europeas y latinoamericanas confiere a esta publicación un carácter verdaderamente internacional, posicionándola como obra de referencia para magistrados, fiscales, abogados, investigadores y estudiantes de posgrado.

Debo indicar que me une una amistad señera, con Bonifacio con todo el aporte que hace a nuestra casa, "La universidad", donde ha formado a hombres y mujeres de derecho, mientras que mi alumno en Maestría Jean Paul, es una muestra clara de trascendencia generacional albergada en **"La Ciudad de la Eterna Primavera"** llamada así o Tacita de Plata", "Capital de la Montaña" o "La ciudad innovadora".

Con la convicción de que el conocimiento jurídico constituye la herramienta esencial para enfrentar la criminalidad tecnológica, y en respaldo institucional a esta segunda edición, suscribe la presente:

Medellín – Colombia, marzo del 2026.

Néstor Posada Arboleda
Rector de la Universidad de Medellín.

PRÓLOGO PRIMERA EDICION

He escrito alguna monografía, muchos artículos en revistas especializadas; he participado en numerosas obras colectivas y soy autor de no pocos prólogos (labor que me resulta especialmente grata). Pues bien, aunque sigo experimentando un cierto gozo, supongo que, como cualquiera, al ver el fruto de mi trabajo en letras de imprenta, algo que otros -quizás pocos- leerán, ninguna sensación es equiparable a la que me asaltó cuando tuve en mis manos el libro que escribí con mi padre. Ni siquiera la igualaba la *primera publicación* que siempre se recibe con impaciencia y se hojea con regocijo. La monografía sobre *Interferencias entre el proceso civil y el proceso penal* que escribimos a medias y que vio la luz en 2002 nos hizo muchísima ilusión. No sé si a mi padre más. Probablemente. No apostaría lo contrario. Mi padre ya estaba jubilado, lo que le hacía disponer de más tiempo. Me apremiaba para acabar ese proyecto común que habíamos emprendido unos años antes. Él había sido Magistrado, dedicado, sobre todo en los últimos años de su vida profesional, al derecho civil. Yo, entonces, era Fiscal: el derecho penal fue siempre el foco principal de mi labor profesional. Aprovechando esas facetas diferenciadas nos pareció una buena idea complementarnos y afrontar esa materia, espinosa y abrupta, formando equipo. Y nos pusimos manos a la obra. Él justo es reconocerlo- con mayor ahínco. Yo tenía la disculpa de la necesidad de compatibilizar con mis tareas profesionales. Un libro escrito a dúo por padre e hijo significa mucho: yo he experimentado esas gozosas sensaciones. Muy orgulloso estoy de ello, como lo estuvo -y estará- mi padre.

Ahora, acogiendo la amable invitación de Bonifacio Meneses Gonzales, amigo y colega, me dispongo a prologar esta monografía sobre Cibercriminalidad que ha escrito con su hijo, Jean Paul Meneses Ochoa, magister en Derecho Penal por la Universidad de Medellín y sus estudios finales de doctor en Derecho por la Universidad Interamericana de la Barra de Abogados de México. ¡Qué satisfacción para padre e hijo! Una satisfacción de la que ya han tenido ocasión de congratularse: es la segunda monografía que corre a cargo de ambos. Antes publicaron otro texto sobre el procedimiento inmediato para investigar y sancionar delitos flagrantes. Es de esperar que se sucedan otros estudios de este tándem "Meneses & Meneses".

Conocí a Bonifacio Meneses Gonzales, aquí en España. Un primer encuentro en Madrid, luego las jornadas anuales "Román García Valera", por invitación del señor alcalde del Ayuntamiento de Sarria, D. Claudio Garrido Martínez, celebradas en la Villa de Sarria, Xunta de Galicia**,** precedió a unas jornadas en

Lima con motivo de una cumbre internacional sobre justicia penal celebrada en aquella Capital y organizada por Poder Judicial de Perú. Esos días compartidos tuve ocasión de comprobar el espíritu acogedor y hospitalario del pueblo peruano plasmado en las atenciones que nos brindaron, entre otros, el magistrado Meneses, siempre servicial. La cumbre, en cuya organización estuvo involucrado, tuvo una altura excepcional. Sobre ciberdelincuencia en la jurisprudencia española versó mi breve disertación. Seguramente esa circunstancia es la que ha movido a los autores a hacerme el honor de prologar esta monografía tarea que encaro con gusto. Así puedo corresponder a esa recepción cordial en el país hermano, y así puedo evocar ese recuerdo de mi padre que no deja de conmoverme.

He hablado de monografía. El término no se adecúa con rigor a lo que espera al lector: es un auténtico tratado de cibercriminalidad. O, mejor, la parte general de un tratado sobre cibercriminalidad que, además, agrupa las diversas perspectivas que confluyen en esa realidad. No es solo dogmática. Los aspectos generales y sociológicos de la sociedad de la información, la criminología de la ciberdelincuencia, los temas procesales y hasta orgánicos y, por supuesto, los aspectos legales, son desmenuzados y desgranados. Un repaso del ambicioso y a la vez detallado y bien sistematizado índice lo pone de manifiesto.

La cibercriminalidad presenta unas características propias que continúan conformándose al impulso del avance de las tecnologías de la información y comunicación (Tics). Han pasado cuarenta años aproximadamente desde que se comenzó a hablar de *criminalidad informática*. Y el término *cybercrime* se acuñó no hace más de treinta años. Pero forma ya parte muy relevante de la realidad criminológica de nuestro mundo. Tanto que algunos estudios revelan cómo crece impetuosamente el porcentaje de población que se siente más expuesta o está más preocupada por ser víctima de un cibercrimen que de un delito tradicional cometido en un espacio físico.

No se trata solo de nuevas formas de cometer los crímenes de siempre. Es algo sustancialmente diferente que no solo ha provocado la necesidad de crear nuevas figuras penales, sino que también obliga a repensar viejas fórmulas necesitadas de adaptación, a explorar otros mecanismos de investigación que necesitan una regulación específica y sin los cuales la sociedad estaría obligada a capitular antes esas nuevas formas de criminalidad, e incluso a alumbrar nuevos derechos fundamentales *(de cuarta generación*, según los catalogan los autores).

Un ejemplo de esto último: el que en la jurisprudencia española está ya consolidado y casi emancipado del derecho a la intimidad y al secreto de las comunicaciones, el derecho al entorno virtual. Es un supuesto paradigmático.

Explorar un smartphone intervenido a un sospechoso no tiene nada que ver con examinar el bloc de notas - ¡o la agenda personal! - que tenía en su, poder. En ambos casos está en juego la privacidad. Pero es claro que las cautelas no pueden ser las mismas. El pequeño dispositivo almacena un volumen de información - sensible y menos sensible- que desnuda a un individuo y que puede convertir la diligencia sin duda en mucho más invasiva que el registro de un domicilio. Se ha hecho necesaria una regulación singularizada de ese nuevo derecho, a caballo entre la privacidad y la autodeterminación informativa.

La necesidad de un abordaje específico es palmaria. La cibercriminalidad, a mi juicio, goza de mayor sustantividad o armazón propio, que otras realidades criminales susceptibles también de estudios específicos: delincuencia económica y empresarial, delitos sexuales.

Aunque han surgido monografías, textos, manuales… sobre ciberdelitos o ciberdelincuencia, no conocía en lengua española un proyecto de abordaje con las dimensiones que se plantean los autores. He manejado algunas muy buenas monografías con una perspectiva criminológica (no puedo dejar de citar a Fernando Miró Llinares); otras con enfoque penal clásico (Eloy Velasco). Pero no se proponen metas tan ambiciosas como las que anima a los autores de esta obra.

Sería absurdo e ingenuo que intentase emularles en este prólogo; tan absurdo como simplón sería que dedicase estas páginas introductorias a ir enunciando los temas que van a abordando perfectamente distribuidos en partes y capítulos. Optaré por, con toda la modestia, plasmar algunas reflexiones propias -en la medida en que podemos hablar de ideas propias: todas son fruto de la metabolización de lo que aprendemos de otros y con este libro se aprende mucho- sobre la materia.

Unas palabras sobre el mapa de la ciberdelincuencia. Creo útil diferenciar entre la versión cibernética de los delitos clásicos (estafa, injurias y calumnias, amenazas, daños…); de aquellos otros que se han creado como consecuencia de fenómenos criminales exclusivos del ciberespacio. Esa diferenciación aparece en algunos lugares de la obra.

Un claro ejemplo de este segundo grupo es la necesidad que surgió de perfilar una infracción específica por la decepción de ver sancionados de forma ridícula a quienes imprudentemente provocaron en Missouri el suicidio de la chica de 13 años, Megan Meier. Había quedado embaucada por un joven, dulce, atractivo, que tocaba muy bien la guitarra y la batería y que le había llegado a seducir a través de una red social. Se mensajearon cordialmente durante tiempo. El joven, Josh Evans, un día, cortó de forma seca con un displicente *el mundo sería mejor sin tía* que había

estado precedido de otros comentarios groseros y nada amables. Poco después la chica se ahorcó con un cinturón en su cuarto. Pues bien, Jhos Evans no existía. Era invención de una mujer de 48 años vecina de la menor que creó al personaje como venganza por las quejas que su hija tenía de los desplantes de Megan y lo puso a interactuar con ella, hasta que entendió que era el momento de provocar el dolor del desprecio

En el Código Penal español en fechas recientes se ha incluido un art. 143 bis tipificando *La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar al suicidio de personas menores de edad o personas con discapacidad necesitadas de especial protección será castigada con la pena de prisión de uno a cuatro años.*

Se trata de un tipo penal emparentado con la inducción al suicidio, pero que tiene unos componentes diferenciados: solo ha surgido la necesidad de una previsión especifica a raíz de la difusión y democratización de las Tics.

Este segundo grupo -delitos específicos, y no versiones de las modalidades clásicas- va creciendo. Echar un vistazo a alguno de los capítulos de esa obra resulta en este sentido muy elocuente: muchos nuevos delitos en cuya etiquetación se ha impuesto una cierta querencia al anglicismo (*stalking, child grooming, sexting, phishing, hackinhg…).*

Pero también los delitos tradicionales, en algunos casos, se ven precisados de adaptaciones como consecuencia del medio comisivo cibernético. Se han hecho indispensables ajustes, retoques o cambios más sustanciales (el delito de daños es un buen ejemplo de ello).

El afán taxonómico por clasificar los *ciberdelitos* a veces se me antoja exagerado. Se corre el peligro de excesos: he visto en alguna publicación hablar de las *ciberlesiones* (¡!). Pero sin duda es necesaria esa clasificación que no eluden los autores (capítulo VII). Antes se ha preocupado de precisar algunos conceptos como la diferencia entre los delitos cometidos a través de la informática y los cometidos contra la informática-, o entre los delitos informáticos y los delitos cibernéticos. Los autores se hacen eco de diversos criterios clasificatorios adoptados por textos u organismos internacionales, o propuestos por la doctrina.

Ha hecho fortuna en algunos ámbitos una clasificación tripartita que distingue entre la ciberdelincuencia intrusiva, la ciberdelincuencia económica y el ciberterrorismo y ciber espionaje.

Cualquiera de los módulos clasificatorios puede ser válido.

El ciberespacio es distinto de los espacios tradicionales. Eso hace mutar no solo la morfología, sino también el contenido del mismo ataque.

En la morfología se aprecian con facilidad esas singularidades: se propicia el anonimato; se puede contactar fácilmente con miles o millones de personas, lo que aumenta las posibilidades de captar ingenuas víctimas; la potencialidad difusiva se incrementa de forma exponencial; las barreras territoriales no existen, lo que dificultará la investigación y la sanción…

Pero también en los contenidos se producen eventualmente variaciones no despreciables. Pienso ahora en las agresiones sexuales *on line*. En la jurisprudencia española existen ya casos de condenas por *ciber violación*. Bajo chantaje y en un contexto virtual el sujeto activo obliga a la víctima a introducirse un dedo en la vagina. La conducta encaja en la descripción típica de la violación, pero se intuye que existe una diferencia no inocua entre la penetración de un miembro corporal propio y uno ajeno. Igual cabe decir de otros delitos sexuales *on line:* es necesario repensar y reordenar. Algún prestigioso Fiscal español ha sugerido la exigencia de interactuación simultánea para poder hablar de delitos de agresión o abuso sexual en un entorno virtual en que, por tanto, no se produce contacto físico. Sin ello, habrá que acudir a otras tipologías (pornografía, exhibicionismo…).

No es lo mismo el ciberespacio. Y por tanto hay que pensar en cada caso las equivalencias con la delincuencia en el espacio físico. No siempre, pero muchas veces es necesario adaptar.

Permítaseme la licencia de ilustras esta idea con una vieja anécdota.

Hace unos años, un día, enfrascado en mis funciones como Fiscal en el Tribunal Supremo, al repasar una causa penal que provenía de Sevilla y se seguía por delitos de falsedad de unos documentos mercantiles me hizo sonreír la imagen castiza que usaba en su declaración ante el Juzgado la víctima. *"¿Las firmas eran falsas?"* se le preguntaba derechamente. Y contestaba con un gracejo que se adivinaba tras el frío texto escrito en papel de oficio: "*Más falsas que un amigo de Facebook"* (se hace fácil representarse la expresión *–feisbuq-* proferida con acento andaluz que zanjaba con rotundidad y con una plasticidad difícil de igualar la eventual duda).

Al igual que no es lo mismo un *amigo* virtual que un amigo *de los de abrazar,* algunas tipologías en el espacio virtual adquieren connotaciones distintas que pueden obligar a remodelarlas o matizarlas.

Precisamente por eso (*no es lo mismo)* me parece muy discutible el refrendo otorgado por el Tribunal Supremo Español a la imposición como pena a un

youtuber que había difundido una acción sobre un indigente que suponía un atentado a su dignidad, de la prohibición de acudir a esa red de videos -*Youtube*- basada en la pena de alejamiento descrita en el Código Penal Español concretable en la prohibición de acudir al lugar del delito durante un tiempo. No. Un espacio o un *sitio* de *internet* no es el lugar en que está pensando el legislador penal al prever esa penalidad.

En materia procesal uno de los campos en que de forma más revolucionaria ha incidido la ciberdelincuencia es en la competencia y en la jurisdicción. Todo un capítulo de la obra analiza esa temática, rica y complicada. El concepto de territorio alrededor del cual se construían los criterios definidores de la jurisdicción y la competencia han saltado por los aires. A nivel nacional e internacional se están reformulando conceptos y buscando novedosos fueros.

Pero no se quedan ahí las especialidades: la prueba de estos delitos y la metodología de investigación -con una importancia redoblada de los mecanismos de cooperación internacional- son objeto de atención detenida en las páginas que siguen.

Y toda esta materia, además, sigue viva: cada año, cada mes, encontramos novedades, tropezamos con realidades que hace unos años nos parecían fantasía.

De la mano de padre e hijo, este libro sirve para profundizar en ese mundo. Ojalá futuras ediciones, que estoy seguro de que llegarán, nos permitan manteneros al día en algo que cambia de forma vertiginosa.

Por mi parte solo me resta agradecer de nuevo esta invitación a introducir un texto de enorme calidad; y, de esa forma, utilizando en sentido figurado un término que tomo prestado del glosario elemental de un usuario informático, establecer un *link* entre mi persona y los autores y su obra. Constituye un privilegio ver mi nombre asociado -*hipervinculado*- con este libro llamado a ocupar por derecho propio un lugar destacado en la copiosa bibliografía producida en los últimos años sobre cuestiones jurídicas surgidas al hilo de la imparable expansión de las nuevas tecnologías.

Antonio del Moral García

Magistrado del Tribunal
Supremo de España. Madrid,
verano de 2023.

PREFACIO

El ciberdelito o los ataques cometidos o facilitados por medio de sistemas informáticos o conductas cometidas a través del ciberespacio son una amenaza creciente y en constante evolución a nivel global, siendo Latinoamérica una de la regiones que registra un mayor crecimiento de las distintas tipologías del ciberdelito en la que países como Perú, se encuentran altamente expuestos a las actividades del crimen organizado transnacional, actualmente especializados en fomentar su modelo de negocio conocido como 'Ciberdelincuencia como Servicio (CaaS)', a través del cual utilizan y ofrecen sus habilidades y destrezas a cualquier persona que esté dispuesto a pagar por ellos o simplemente para compartir ganancias con otros grupos delictivos. A través de este modelo de negocio, los delincuentes explotan, intercambian y comercializan todo tipo de actividades ilícitas, desde venta y renta de botnets, herramientas para crear ataques sobre denegación de servicio (DDOS), creación de malware, troyanos y phishing para dirigir ataques de Ransomware y para cometer fraudes y estafas, venta y alquiler de dispositivos para desbloquear contraseñas y medios de pagos digitales, alquiler de programas para el intercambio de imágenes y contenido de explotación sexual de menores, hasta servicios más sofisticados como la comercialización y explotación del uso de mezcladoras (cryptomixers) para el intercambio y mezcla de criptomonedas con dinero con el fin de facilitar el blanqueo de capitales derivados de actividades ilícitas, y evitar ser identificados y perseguidos por las autoridades ejecutoras del sistema de justicia.

De acuerdo con Statista, Perú se encuentra en el cuarto lugar de los países que más ciberataques recibieron durante 2020, una tendencia que seguramente seguirá incrementándose en los próximos años, y en la que las autoridades del sistema de justicia tienen la nada fácil tarea de responder a las demandas de los ciudadanos para protegerlos en contra de las actividades delictivas cometidas a través de sistemas informáticos o facilitadas a través del ciberespacio.

En Perú, como en la gran mayoría de los países de la región, cada vez es mayor el índice de personas que son víctimas de nuevas modalidades de ciberdelincuencia, tales como ciberviolencia (sexting, pornovenganza, difusión de imágenes sexuales no consentidas, cyberbullying), el uso y difusión de sistemas de Inteligencia Artificial a través de los ultra falsos (deepfakes) para lograr suplantar la imagen, voz e identidad de personas, defraudar y causar daño a la imagen y reputación de mujeres, adolescentes y menores de edad, entre otras modalidades que se encuentran en constante evolución.

La obra que ahora ustedes tienen en sus manos, es un esfuerzo ampliamente destacable de dos expertos nacionales del ámbito jurídico penal en Perú. El libro aborda en diversos capítulos y artículos y desde distintas perspectivas, la clasificación de conductas y tipologías del ciberdelito, las estadísticas y datos sobre cibercriminalidad en Perú, aspectos criminológicos del ciberespacio, las principales leyes y tratados internacionales y regionales aplicables a la investigación del ciberdelito, la labor de los organismos internacionales en la lucha contra la cibercriminalidad, aspectos procesales del ciberdelito, la temática de la jurisdicción aplicable, la valoración de la evidencia por los tribunales nacionales, el rol de las autoridades nacionales y del Poder Judicial encargadas de la investigación y su respectivo marco normativo, aspectos de asistencia y cooperación internacional, así como las redes de fiscales existentes encargadas de cooperar en la investigación de ciberdelitos y la preservación de evidencia con otros países.

La obra destaca las principales problemáticas y retos a los que se enfrentan en la práctica los fiscales, jueces y magistrados para investigar, procesar y adjudicar en forma más efectiva los ciberdelitos en el ámbito nacional.

Auguro que este libro será un gran aporte no solamente a la amplia literatura académica que ya existe sobre la materia en Latinoamérica, sino que será sumamente útil para el intercambio de experiencias prácticas nacionales entre abogados postulantes en materia penal, así como una herramienta muy útil de apoyo en la labor de los jueces, magistrados y fiscales de otros países de la región encargados de la compleja tarea de la investigación y adjudicación del ciberdelito en sus respectivas jurisdicciones.

En hora buena a los autores Jean Paul Meneses, joven investigador del derecho y va por su tercera publicación y especialmente mi más cordial agradecimiento al Juez Bonifacio Meneses González, amigo y profesional sumamente comprometido en fomentar y crear la especialización de los jueces en materia de ciberdelito y evidencia electrónica en ese lindo y cálido país que es Perú.

Dr. Cristos Velasco San Martín

Consultor y Formador en Ciberdelito, Ciberseguridad e Inteligencia Artificial,
Docente en la Universidad Estatal Duale Hochschule Baden-Württemberg,
(DHBW) en Mannheim y Stuttgart, Alemania.

Mannheim, Alemania, marzo de 2024.

PRESENTACIÓN

Para el Instituto Iberoamericano de Justicia constituye un motivo de satisfacción y de fundamentado orgullo el presentar a la comunidad jurídica de la Región y a la sociedad en su conjunto esta magnífica obra de los juristas doctores Bonifacio Meneses González y Jean Paul Meneses Ochoa; padre e hijo en una continuidad existencial y académica que exalta al mismo tiempo el pensamiento y el afecto.

En la ya característica académica que es la suya, los autores se sumergen en los temas de actualidad y se adelantan a examinar los escenarios futuros que esta actualidad nos propone, ensayando soluciones, proponiendo respuestas y cultivando consciencia en este caso sobre un fenómeno no tan reciente pero además no suficientemente examinado, al menos no en la dimensión que este verdadero tratado no propone.

Esta obra de relevancia jurídica y social, impregnada de modernidad y con visión de futuro, propone un análisis exhaustivo sobre la cibercriminalidad, abordando el tema desde múltiples perspectivas que incluyen la criminológica, la política-criminal, la dogmática, la procesal y la de cooperación internacional.

Para ello, el lector no está solo frente a esta abrumadora cantidad de nuevas formas, conceptos, tendencias y choques que el derecho enfrenta, los autores guían al lector en este mundo novedoso para que su comprensión sea extrema pero además para invitar a la sociedad, a palpar de primera mano los fenómenos a los que aquella y el derecho penal se enfrentan ante la evolución de la criminalidad informática y la necesidad de adaptarse a las nuevas formas de delitos en el mundo digital, enfatizando la importancia de la colaboración entre diferentes entidades y países para combatir eficazmente estos delitos.

A través de esta obra, los autores elaboran provocan una dinámica colaborativa entre sus experticias que permite adentrarse en la complejidad de la cibercriminalidad, resaltando la necesidad de una constante actualización en las estrategias de prevención y persecución, así como la importancia de la capacitación y el desarrollo normativo que analiza las experiencias de expertos de diversos países.

Con la finalidad de darle aún más elementos de análisis al lector, los autores proponen aspectos de relevancia procesal como el estudio de la prueba electrónica y la evidencia digital en el proceso penal, subrayando cómo su

correcto tratamiento y admisibilidad son cruciales para la resolución de casos de ciberdelitos.

La propuesta de la obra no se limita a un análisis descriptivo de la problemática vigente, conceptos, análisis estadísticos y comparados, además hace énfasis en la implementación de medidas y reformas legales para enfrentar la cibercriminalidad en el sistema penal peruano y en la Región, presentando un estudio detallado sobre el tema desde diferentes ángulos y proponiendo mejoras para la lucha contra este tipo de delitos.

Un fenómeno de este nivel no omite recordar la importancia de la cooperación judicial internacional, destacando el papel del Convenio de Budapest y la necesidad de mecanismos formales e informales para facilitar la obtención de evidencia y la persecución de delitos informáticos. Además, se aborda la evolución del derecho informático y la ciberseguridad, discutiendo cómo la protección de los bienes jurídicos en la era digital y la historia del internet han impactado en la legislación y las políticas públicas para mejorar la calidad de vida y prevenir el delito.

Este análisis multidisciplinario pone en evidencia lo enriquecedor que resultará para el lector llevar a sus manos un libro que aborda con tecnicismo y precisión la complejidad de la cibercriminalidad y subraya la importancia de una respuesta integrada que incluya actualizaciones legislativas, cooperación internacional, y especialización judicial para combatir eficazmente los delitos informáticos.

La obra se destaca por su enfoque multidisciplinario y exhaustivo hacia el fenómeno de la delincuencia digital, evidenciando un profundo entendimiento y análisis de la materia desde diversas perspectivas que incluyen la criminológica, la política-criminal, la dogmática, la procesal y la cooperación internacional. Este enfoque holístico no solo demuestra la complejidad del tema abordado sino también la capacidad de los autores para integrar distintas disciplinas en el estudio de la cibercriminalidad, lo que sugiere una profunda erudición y un compromiso con la comprensión integral del tema.

Nos encontramos entonces, ante un verdadero tratado sobre la cibercriminalidad que aborda la temática desde una perspectiva actualizada, comparada y atractiva, incorporando las últimas tendencias y desafíos que enfrenta la sociedad en relación con los delitos informáticos.

La inclusión de temas como la autoría y participación en los ciberdelitos, así como la tipicidad subjetiva en el ciberdelito, muestra un enfoque detallado y

específico hacia aspectos clave que definen la naturaleza y el procesamiento de los delitos digitales en el marco legal actual.

Esta atención a los detalles y la profundidad en el tratamiento de temas específicos subrayan la meticulosidad de los autores en su análisis y su deseo de proporcionar una comprensión exhaustiva y matizada de la cibercriminalidad, lo que es esencial para abordar efectivamente este fenómeno en constante evolución.

En estos tiempos que son los nuestros, de vertiginoso desarrollo de las tecnologías de la información, que han revolucionado la interacción humana, que son fuente de riqueza y conocimiento, y, a la vez causa de riesgos y daños, la lectura y estudio de la obra que hoy presentamos es simplemente obligatoria, para el jurista en permanente actualización, para el estudiante con visión o simplemente para quienes quieran comprender de mejor manera los desafíos del derecho y la seguridad en clave de ciberespacio.

Es motivo de orgullo para el Instituto Iberoamericano de Justicia que uno de sus miembros nos distinga con la producción de esta obra en compañía de otro reconocido jurista peruano en cuyas venas corre la misma inteligencia, rigurosidad académica y pasión por el Derecho que su progenitor.

Resulta entonces necesario reconocer, agradecer y felicitar este trabajo de enorme actualidad y trascendencia para la ciencia del Derecho.

Gustavo Jalkh Röben, PhD

Presidente del Instituto Iberoamericano de Justicia

INTRODUCCIÓN A LA SEGUNDA EDICION

Parece ayer que, gracias a la Pontificia Universidad de Salamanca, iniciamos el peregrinaje en la difusión y presentación de la Primera Edición de esta gesta jurídica llamada libro, en ese trajín hemos conocido a dignas personas y lugares esplendidos donde fue presentado y debatido cada uno de los presupuestos enunciados en el flagelo llamado Ciber crimen.

En efecto, la presentación del libro en el **Ateneo de Madrid** que posee una historia estrechamente ligada a la evolución del pensamiento liberal, científico y cultural de España desde el siglo XIX hasta la actualidad, Fundado en **1835** con el nombre de **Ateneo Científico y Literario**, nació en el contexto de la España liberal como un espacio de **libertad intelectual, debate crítico y formación ciudadana**. Desde sus inicios se concibió como una institución privada, independiente y abierta, dedicada a la promoción de la ciencia, las letras, el derecho, la filosofía y las artes.

A lo largo de su historia, el Ateneo ha sido un auténtico **laboratorio de ideas** y un escenario clave de la vida intelectual española. Por sus tribunas y salones pasaron figuras fundamentales como **Benito Pérez Galdós, Ramón y Cajal, Miguel de Unamuno, José Ortega y Gasset, Manuel Azaña**, entre muchos otros, así como científicos, juristas, escritores y pensadores iberoamericanos y europeos. Durante distintas etapas políticas monarquía, república, dictadura y democracia, el Ateneo mantuvo su vocación de **pensamiento plural y espíritu crítico**, sufriendo cierres y restricciones en épocas de represión, pero recuperando siempre su papel central en la vida cultural española.

A lo largo del tiempo, el Ateneo ha tenido diversas sedes, reflejo de su crecimiento y consolidación institucional:

- **Primeras sedes (siglo XIX)** En sus años iniciales, el Ateneo funcionó en locales provisionales del centro de Madrid, adaptados a sus actividades académicas y culturales, mientras se consolidaba como institución.
- **Sede definitiva – Calle del Prado (desde 1884):** En **1884** se inauguró su sede actual, ubicada en la **Calle del Prado n.º 21**, en el denominado **Barrio de las Letras**. Este edificio histórico se convirtió en un símbolo del Ateneo y del Madrid intelectual.

La sede alberga espacios emblemáticos como:

- La **Biblioteca del Ateneo**, una de las más importantes bibliotecas privadas de España.
- El **Salón de Actos**, escenario de conferencias históricas.
- Salas de exposiciones, tertulias y secciones especializadas.

Hoy, el Ateneo de Madrid sigue siendo un **referente cultural y académico**, manteniendo viva su misión fundacional: servir como espacio de encuentro para el pensamiento crítico, el diálogo interdisciplinario y la proyección cultural de España hacia Europa e Iberoamérica, fiel a una tradición de casi dos siglos al servicio del conocimiento y la libertad intelectual. En ese marco impresionante, hicieron uso de la palabra el prologuista Antonio del Moral, digno magistrado del Supremo Tribunal de Justicia del reino de España, el maestro Manuel Lázaro Pulido, Profesor de Derecho y Filosofía de la Pontificia Universidad de Salamanca, la Dra. Rosa María del Carmen Tome García, magistrada de la Audiencia Nacional, querida Rosita, entrañable amiga y mejor persona, además de los autores, la crema y nata de la juridicidad Madrileña se dio cita a tan magno evento, noche de gloria y agradecimiento infinito a los organizadores.

En fechas anteriores y posteriores al Ateneo, el libro fue presentado en diferentes estadios dedicados a lo profundo y arraigado espíritu académico, para ello viajamos los autores cargando más que el libro hecho en España, ilusiones y deseos que pueda servir a los lectores en el mejor conocimiento de la ciber seguridad y como no la ciber delincuencia como fenómeno global y existencial.

En la madre patria, además, tuvimos la oportunidad de participar en un evento que corrobora todas nuestras expectativas de ciber seguridad y ciber delincuencia, que viene a ser un **proyecto de ciberseguridad de la Policía Nacional de España (C1b3rWall)**, que ofrece formación y conciencia digital, que proporciona servicios de protección digital, o de forma más general, a la idea de un **muro de seguridad en el ciberespacio** para proteger redes y datos. Una iniciativa nacida en 2018 para promover la ciberseguridad y la capacitación digital en España.

Este evento de polendas se llevó a cabo en la bella ciudad de Ávila en España, en la Academia de Policía, en dicho lugar advertimos que se trata de un centro de formación intensiva que prepara física, mental y éticamente a los futuros agentes, combinando entrenamiento riguroso (tiro, conducción, defensa) con instrucción teórica (leyes, criminología, protocolo) en un ambiente

disciplinado, forjando el carácter y la vocación de servicio, con instalaciones que incluyen aulas, gimnasios y campos de tiro, y una duración variable según el país, preparando líderes para la seguridad ciudadana con un enfoque en el desarrollo de competencias especializadas y valores como el honor y el compromiso.

Creemos sin lugar a dudas que es el lugar perfecto y mejor desarrollado del debate de ciber seguridad y ciber crimen del mundo entero, satisfechos enteramente por las conclusiones y mejor entendimiento de este problema de envergadura mundial.

Punto de realce, histórico para nosotros, participar en Los días 29 y 30 de mayo, en la isla de Ibiza al **congreso sobre Inteligencia Artificial y Derecho** que reunió a conocidos expertos en la materia. El evento se trasladó al Insotel Fenicia Prestige, nuestro agradecimiento a Diego Castro, de CVC Orión Business & Law School, entre las expositoras fu Dolores Chaplin, nieta del conocido cómico, quien habló del uso de la IA en creaciones cinematográficas actuales, lo que ha generado un serio problema para familias como la suya.

A su vez tuvimos a bien escuchar a Juli Ponce Solé, doctor en Derecho y catedrático de Derecho administrativo en la Universidad de Barcelona. También, el prestigioso analista económico Marc Vidal y el director de cine nominado a los Goya, Marcos Cabotá. En consecuencia, la visita a España fua altamente satisfactoria en todos los sentidos.

Culminado ese evento impresionante, nos trasladamos a S**arria** es un municipio y localidad española de la provincia de Lugo, en la comunidad autónoma de Galicia. Es capital de la comarca de Sarria, es conocida por ser el punto de inicio habitual para realizar los últimos 100 km del Camino de Santiago francés. Entre sus monumentos destaca la torre de la fortaleza de los Marqueses de Sarria, único elemento superviviente de la fortaleza, y el monasterio de la Magdalena construido en el siglo XIII. En total, en todo el municipio se pueden encontrar hasta 20 iglesias de la época románica.

"La XVIII JORNADA JURIDICA Roman Garcia Valera", tuvo el año próximo pasado un éxito fabuloso, inaugurado por el Dr. Pascual Sala Sánchez Ex - presidente del Tribunal Constitucional – luego contamos con la participación y ponencias de los maestros. Virgilio Zapatero Gómez, ex - ministro de Relaciones con las Cortes. Catedrático de Filosofía del Derecho en la Universidad de Alcalá. Edward Martin Regalado, de Regalado & Galindo Abogados. La Dra. Isabel Perelló Doménech. Presidenta del Consejo General del Poder Judicial, el distinguido y gran amigo Don Claudio Garrido Martínez. Alcalde de Sarria, José María Gómez y Díaz-Castroverde. Presidente del

Tribunal Superior de Xustiza de Galicia, el Dr. Francisco Marín Castán Expresidente del Tribunal Supremo, el Dr. Juan José González Rivas Ex - presidente del Tribunal Constitucional - el Dr. Rafael Mozo Muelas Ex - presidente del Consejo General del Poder Judicial, la Dra. María Emilia Casas Baamonde, ex - presidenta del Tribunal Constitucional. La presencia del Dr. Cándido Conde Pumpido. Presidente del Tribunal Constitucional, un sabio que asi es considerado, su charla amena su amistad sincera, inolvidable don Juan Antonio Xiol Ríos, ex - vicepresidente del Tribunal Constitucional, la Dra. María del Pilar Teso Gamella, magistrada de la Sala 3ª del Tribunal Supremo, fue digno y de satisfacción personal tener en el podio a un dilecto y querido amigo el Dr. Jordi Nieva-Fenoll, catedrático de Derecho Procesal de la Universidad de Barcelona, luego el Peru estuvo presente con el co autor quien presentó este trabajo y fue reiteradamente comentado en ese paraninfo inolvidable de honor, muchas gracias al selecto ambiente y mejor podio de Europa.

Colombia fue un paradero obligatorio por la magnitud, excelencia académica como crisol de grandes hombres de derecho, más aún que el co autor Jean Paul, es magister de la mejor casa de estudios de nuestro vecino y hermano país, además que el co autor Bonifacio es docente de esa digna casa de estudios. Nos albergó la **Feria Internacional del Libro de Medellín** la misma que se ha consolidado como uno de los **eventos culturales y editoriales más importantes de Colombia y de América Latina**. Desde su creación, ha sido un espacio privilegiado para la **promoción de la lectura, el diálogo intercultural y la circulación del pensamiento académico, literario y científico**, integrando a autores, editores, investigadores y lectores de diversas partes del mundo.

Este encuentro anual no solo celebra el libro como objeto cultural, sino que lo proyecta como **herramienta de transformación social**, coherente con la vocación de Medellín como ciudad comprometida con la educación, la cultura y la innovación. La feria destaca por su **programación plural**, que articula literatura, derecho, ciencias sociales, derechos humanos, memoria histórica y debates contemporáneos de alcance regional e internacional.

Asimismo, la Feria Internacional del Libro de Medellín cumple un rol estratégico en la **integración iberoamericana**, al facilitar el intercambio de ideas entre autores latinoamericanos y europeos, fortaleciendo redes académicas y culturales. Su impacto trasciende el ámbito editorial, convirtiéndose en un **escenario de reflexión crítica, construcción de ciudadanía y democratización del conocimiento**, reafirmando el papel del libro como pilar del desarrollo cultural y social.

La **Feria Internacional del Libro de Medellín** ha sido escenario de presentación de obras de **destacadas personalidades del ámbito literario, académico, científico y cultural**, consolidándose como un espacio de referencia para el pensamiento latinoamericano y universal.

A lo largo de sus ediciones, la feria ha contado con la presencia de **escritores de reconocimiento internacional**, premios literarios, intelectuales, ensayistas, historiadores, juristas y científicos sociales, tanto de Colombia como de otros países de América Latina, Europa y Norteamérica. Autores de la talla de **novelistas consagrados, poetas influyentes, académicos de prestigio y líderes de opinión** han elegido este espacio para dialogar con el público y presentar sus más recientes obras.

Asimismo, la feria ha dado cabida a **figuras del pensamiento crítico y de las ciencias sociales**, cuyas publicaciones abordan temas como derechos humanos, memoria histórica, justicia, democracia, violencia, cultura y transformación social, reforzando el carácter plural y reflexivo del evento.

Esta confluencia de personalidades ha convertido a la Feria Internacional del Libro de Medellín en un **punto de encuentro intelectual de alto nivel**, donde el libro se proyecta no solo como expresión artística, sino también como instrumento de análisis, debate y construcción de ciudadanía, fortaleciendo su prestigio en el ámbito iberoamericano.

No podemos dejar de agradecer al señor Rector de la Universidad de Medellín y presentador de la actual edición Néstor Posada Arboleda, al Dr. Ricardo Asturio Gil Barreda, destacado docente y jefe de la División de Publicaciones de tan importante casa de estudios y a un hermano de elección David Gutiérrez Castaño, director de la escuela de pos grado, quien tuvo la bondad de presentar el libro y darnos la posibilidad de ser docentes y sobre todo presentarnos en la Feria Internacional, no tenemos palabras para agradecerle tamaño gesto y las veces que vino a Perú a capacitar a los jueces y fiscales del Perú, gracias Deivi entrañable personaje que ya es parte de nuestra familia.

La universidad católica de Cuenca – Ecuador, **(UCACUE)** constituye una de las instituciones de educación superior más relevantes del Ecuador, reconocida por su **compromiso con la formación integral**, la excelencia académica y la proyección social, inspiradas en los valores del **humanismo cristiano**.

En el ámbito del **Derecho**, la Universidad Católica de Cuenca ha desarrollado una labor sostenida en la **formación de juristas**, promoviendo el

rigor científico, la ética profesional y la defensa de los derechos fundamentales. Sus programas jurídicos se caracterizan por articular la **teoría con la práctica**, el análisis crítico de los sistemas normativos y la atención a los desafíos contemporáneos de la justicia, tanto a nivel nacional como regional.

Las **autoridades universitarias**, y en particular el **Rector**, cumplen un rol central en la conducción académica e institucional, orientando a la universidad hacia estándares de calidad, investigación y vinculación con la sociedad. Bajo su liderazgo, la UCACUE ha fortalecido su presencia académica, impulsando el diálogo interdisciplinario, la cooperación internacional y el posicionamiento de la Facultad de Derecho como un espacio de reflexión jurídica y compromiso social.

En conjunto, la Universidad Católica de Cuenca y sus autoridades representan un **referente académico y ético** en la formación jurídica, contribuyendo al fortalecimiento del Estado de derecho y al desarrollo de una cultura jurídica comprometida con la justicia y la dignidad humana.

Digno lugar que gracias al señor presidente del Instituto Iberoamericano de Justicia Gustavo Jalkh Roben, pudo ser posible la presentación de este documento académico, para dicha actividad no podían faltar, el vicepresidente del IIBJ, el excelentísimo señor doctor don Tomas Montero Hernanz, (esa exigencia de presentación lo pinta de cuerpo entero a este jurista Vallisoletano), a su vez del director y caro amigo Tomas Alvear Peña, como del jurista "Tico" Mauricio Garro Guillen.

En México, la presentación igualmente fue apoteósica El **Castillo de Chapultepec**, ubicado en la Ciudad de México, es uno de los **espacios históricos y culturales más emblemáticos del país y de América Latina**. Con una trayectoria que se remonta al siglo XVIII, ha sido escenario de acontecimientos decisivos de la historia mexicana y hoy alberga el **Museo Nacional de Historia**, convirtiéndose en un símbolo de **memoria, identidad y proyección cultural**.

Que el **Castillo de Chapultepec** haya sido **lugar de presentación de nuestro libro** reviste un significado académico y simbólico de especial relevancia. Se trata de un recinto que ha acogido expresiones culturales, intelectuales y artísticas de alto nivel, y cuya vocación trasciende lo histórico para consolidarse como un espacio de **difusión del pensamiento y diálogo entre naciones**.

La presentación de la obra en este escenario histórico inscribe nuestro trabajo dentro de una **tradición de reflexión crítica y aporte al conocimiento**, otorgándole una proyección iberoamericana y un reconocimiento que refuerza su valor académico. El Castillo de Chapultepec, con su legado y prestigio, se convierte así en un marco excepcional que realza la trayectoria del libro y de sus autores, vinculándolo con un espacio que representa la **continuidad entre historia, cultura y pensamiento contemporáneo**.

Es importante destacar que la **Universidad de la Barra de Abogados de México** tuvo un rol fundamental al **hacer posible la presentación de la obra en el Castillo de Chapultepec**, uno de los recintos históricos y culturales más emblemáticos de México y de América Latina.

Esta decisión institucional refleja la **apertura académica, el compromiso cultural y la visión jurídica internacional** de la Universidad, al vincular la reflexión contemporánea sobre la **cibercriminalidad** con un espacio de alto valor histórico y simbólico. Gracias a este respaldo, la obra pudo proyectarse en un escenario que trasciende lo académico para insertarse en la **tradición cultural y jurídica del país**.

La iniciativa de la Universidad de la Barra de Abogados de México no solo realzó la presentación del libro en su local institucional, sino que también reafirmó su papel como **promotora del pensamiento jurídico innovador**, del diálogo iberoamericano y de la difusión del conocimiento jurídico en espacios de máxima relevancia histórica y cultural.

Mientras que en nuestro país, la presentación en familia de este libro en su primera edición se llevó a cabo en las instalaciones de la Universidad "San Ignacio de Loyola" USIL es una universidad reconocida en Perú, destacando en rankings nacionales e internacionales por su calidad educativa, investigación e innovación, ubicándose frecuentemente en el Top 5 o Top 8 de universidades privadas en el país según QS y SUNEDU, con énfasis en formación empresarial y desarrollo sostenible, aunque la percepción puede variar según el programa específico y las prioridades del estudiante.

Ahí con la presencia del señor presidente del Instituto Iberoamericano de Justicia, Gustavo Jaklh Roben, de nuestro director del IIBJ Carlos Tomas Alvear Peña, fue muy satisfactoria no solo en su contexto sino en la propia presentación como el discurso dado por el distinguido expositor Dino Carlos Caro Coria, sin lugar a dudas este acto académico fue muy comentado en las redes sociales como en la colectividad jurídica del Perú y del mundo entero. Nuestro agradecimiento al Dr. Justo Balmaceda Quiroz, compañero de ILEA

Roswell – EEUU, quien fue un dilecto anfitrión, asimismo desde España vino a presentar este libro el Maestro Fernando Molina, Decano de la Unidad de Pos grado de la Universidad Autónoma de Madrid.

Otro gesto de plena satisfacción fue la presentación del libro en la bella ciudad de Arequipa, en horas de la mañana en el auditorio "Álvaro Chocano Marina", con los juristas Roger Pari Taboada y Nicolas Iscarra Pongo, presidente de la Corte Superior de Justicia, que satisfacción hacer ese periplo jurídico, nuestro reconocimiento a la Dra. Sonia Acero, funcionaria de tan noble Corte, que a nuestro concepto es el motor esencial en la noble Corte Superior de Arequipa, en seguida nos trasladamos a las instalaciones del Ilustre Colegio de Abogados de Arequipa, donde su Decano John Michael Mesías Romero, dio las palabras de presentación y ofrecimiento de este libro en su primera edición mil gracias señor Decano, en horas de la tarde el señor Presidente de la Junta de Fiscales Superiores de Arequipa, Dr. Ciro Alejo Manzano, hizo la presentación de nuestro trabajo, haciendo votos por la difusión y extensión de trabajos de investigación sobre la materia, nuestro dilecto paisano y amigo hizo una semblanza de nuestra amistad y recorrió hoja a hoja el libro cuyo acto nos hizo digna la capital jurídica del Perú.

Días después, viajamos a la ciudad de Puno, donde el señor Decano del Ilustre Colegio de Abogados de Puno, nos permitió ofrecer a la comunidad jurídica lacustre este trabajo que conforme a lo expresado resulta de mayor compromiso de retornar a la tierra donde Dios nos diera la vida y vimos por primera vez la luz de ese sol maravilloso que diariamente sale de las fulgurantes aguas del majestuoso lago sagrado de los Incas, el Titicaca de donde emergieron la pareja mítica Manco Cápac y Mama Ocllo, fundadores del gran imperio de los incas, ahí donde cursamos los estudios iniciales, primarios y secundarios con un excelente grupo humano dentro de los cuales siempre reconocido al doctor Felipe Carpio Miranda, amigo de la cuna y conservamos la amistad imperecedera como colegas, en tal sentido esa actividad académica tenía ribetes de sensibilidad y razonamiento en la esperanza que el trabajo presentado contenga los cimientos inmarcesibles de esa roqueña cultura, siempre dando homenaje a don Juan Meneses Diaz, padre y abuelo de los autores que formó ese espíritu de sacrificio como de lucha constante.

En ese periplo la Municipalidad de la Provincia de San Román – Juliaca y la Corte Superior de Justicia de Puno, hicieron posible la ceremonia en el paraninfo de la Municipalidad de Juliaca, por ello no podemos dejar de agradecer al señor magistrado Javier Arpasi Hallasi, Juez Superior y mejor amigo, al doctor Youl Riveros Salazar Juez Penal y al señor Presidente de la Corte Superior de

Justicia, Beny Álvarez Quiñonez, con quien hicimos los recuerdos de haber laborado como Trabajador de Servicio II y luego como Juez Superior Titular y Presidente de la Honorable Sala Penal.

El presente trabajo fue madurando en cada presentación y el apoyo de la colectividad jurídica peruana, es así que al llegar a Tacna donde la señora presidenta Rosa Juárez Ticona, hizo los comentarios a la presentación del documento literario jurídico, muchas gracias a la Corte Superior de Justicia de Tacna, igualmente al Ilustre Colegio de Abogados de Tacna y como no dos sesiones de trabajo en la Universidad Privada de Tacna, **Rector:** Dr. Hugo Cirilo Calizaya Calizaya. **Vicerrector Académico:** Dr. Arcadio Atencio Vargas. **Vicerrector de Investigación:** Dr. Elmer Marcial Limache Sandoval y el señor Decano de la facultad de derecho, Rafael Supo Hallasi, especial mención al señor Juez Pedro Franco Apaza, formadores de formadores de ETI PENAL, profesor de esa noble casa de estudios y mejor amigo, la presentación de nuestro libro en su primera edición fue un éxito rotundo en cada lugar donde fue ofrecido a la comunidad jurídica.

Merece especial atención haber colocado en sumo grado este trabajo en la "Ciudad del eterno sol" la tierra de la "Huacachina" el soleado paraje que bendice el "El Señor de Luren", lugar donde el co autor fue presidente de la Corte Superior de Justicia de Ica, la ceremonia que inicialmente organizó el Sindicato de Trabajadores de dicho distrito judicial, concitó el apoyo e interés de todas las autoridades locales, desde el Alcalde, Presidente Regional, Presidente de la Corte Superior de Justicia, funcionarios de todas las dependencias del Estado y como no la comunidad Jurídica, en dicho evento estuvo también el Instituto Iberoamericano de Justicia, representado por su Director Ejecutivo, Tomas Alviar Peña, conjuntamente con la Dra. Alexandra Domínguez, juez laboral de Quito Ecuador y los expositores peruanos Sánchez Porturas y Rocío Quilca Molina distinguidos magistrados que dieron realce a dicho acto académico.

Ahora bien, para fortalecer el complejo mundo del ciber crimen y establecer nuevos criterios en su lucha a través de la **ACADEMIA PERUANA DE CIBER SEGURIDAD Y DERECHO PENAL INFORMATICO,** presidido por el co autor Jean Paul Meneses y el patrocinio de tan importante institución hemos visto como se ha fortalecido la organización de eventos académicos propios del tema, en la Corte Superior de Justicia de Lima, tanto así que el "Primer Congreso Internacional de Ciber Crimen, nuevas tecnologías e inteligencia artificial fue considerado como uno de los mejores del mundo pero único en el Perú, nuestro agradecimiento al señor Juez Supremo Titular Víctor

Prado Saldarriaga, presidente de la Sala Penal de la Corte Suprema de Justicia de la República, como a los señores expositores nacionales y extranjeros Aurora Remedios Fátima Castillo Fuerman **Fiscal Superior de Ciber Delincuencia.** los señores docentes especialistas en Ciber criminalidad, Dino Carlos Caro Coria, Ricardo Elías Puelles**,** Mario Yunis Arroyo – Ing. Especialista en ciber seguridad e inteligencia artificial a los maestros, Cristos Velasco San Martin de la Universidad de Manheim, Alemania, María de Lourdes Gutiérrez Ortiz Monasterio – Secretaria de las Naciones Unidas para Ciber Crimen para el Caribe y Centro América, Rosa María Tome García, Magistrada de la Audiencia Nacional del Reino de España, Antoni Bosch Pujol,

Director General (CEO): Institute of Audit & IT-Governance (IAITG). Data Privacy Institute (DPI) dentro del ISMS Forum. Docente de Pacífico Business School, Centrum-PUCP (Perú) y Universidades en España, Luis Carlos Caballero Caballero, Inspector General de la Policía Española, Carlos Tomas Alvear Peña, secretario ejecutivo del Instituto Iberoamericano de Justicia, Julio Aguayo Urgiles, ex Presidente de la Corte Superior de Justicia de Guayaquil,, Daniel Dupuy Directora del Observatorio de Ciber crimen de Argentina y docente de la Universidad Austral, Juan Carlos Carretero, ex Decano de la facultad de derecho de la Universidad de Matanzas en Argentina, Mauricio Garro Guillen, ex Director de la Oficina de Preservación de Datos de Costa Rica; Luis Jorge Gamboa Olea, Presidente del Tribunal Superior de Morelos México, David Gutiérrez Castaño, Director de la Escuela de Pos grado de la Universidad de Medellín, los profesores Chileno Jaime Verga Vega y Laura Mayer Lux.

Es preciso señalar y agradecer al Dr. Luis López Oliva, destacado hombre de derecho de Guatemala y caro amigo, quien organizó la difusión y presentación de este trabajo en Guatemala, reunión académica que tuvo que realizarse en forma virtual, pero contó con la presencia de grandes juristas y amigos entrañables como la Dra. Karoll Pérez, presidenta del Tribunal de feminicidio de Guatemala, la Dra. Rosemary López, Nelly Mejicano juristas de época.

Finalmente hacemos votos para que este año, podamos recorrer nuevamente en el peregrinaje maravilloso de difundir estas líneas y pongamos en relieve que este nuevo flagelo tienes formas de combatir, con estas armas que el derecho nos da, es la capacitación constante decidida y pragmática.

Agradecemos al Instituto Iberoamericano de Justicia por su apoyo constante a la difusión de este trabajo, a la Dra. Catalina Stroe, coordinadora de

Glacy e del Consejo de Europa por todo el apoyo en favor de la capacitación de este tema tan delicado para el mundo entero.

En esta segunda edición, queremos que colme las expectativas que en la primera edición fueron ausentes, nuestro eterno agradecimiento a nuestro prologuista Manuel Lazara Pulido, quien, a través de la Universidad Pontificia de Salamanca, hace posible esta publicación.

Gracias al señor y querido amigo Antoni Bosch Pujol, quien desde el primer día que nos conocimos hicimos el inicio de una gratísima amistad que se trasunta en sus letras, de igual manera a nuestra maestro y amigo Néstor Posada Arboleda, Rector de la Universidad de Medellín quien acepto en el acto hacer la presentación de esta Segunda Edición, por tanto nos llena de orgullo la confianza que le dieron a la primera edición, texto que se agotó en sus ventas en España, Ecuador, Colombia, México y Guatemala.

En definitiva, nuestra vocación y afecto al Derecho se debe al patriarca de la familia Bonifacio Meneses Romero, que inspiró a sus nietos Gloria Rosario, Roger Fernando, Estela Rosemary a darnos las pautas para abrazar esta noble carrera, a sus bisnietos, Luis Miguel, Fiorela Natali, Betty Victoria, Jean Paul, Jeffer y María Belén, todos en el tándem Meneses & Meneses, a quienes hacemos el homenaje con estas líneas.

Lima, verano del 2026.

Los autores.

AGRADECIMIENTOS

A mis padres Juan (+) y Victoria, por darme la vida y ser el faro que oriento mi existencia hacia el derecho y la justicia.

A mis hermanos Eva, Juan Miguel, Belia Marlene y colegas Gloria Rosario, Roger Fernando y Estela Rosemary

A mis adorados hijos por su constante apoyo y comprensión del tiempo que les resté para dedicárselo al Derecho, Jean Paul, Jean Pierre Humberto, Blanca Victoria, Kiara Caroline (+), María Belén, Kathia Ginela y Guadalupe.

A mis colegas y amigos donde preste servicios, desde hace 43 años en el Poder Judicial, Corte Suprema de Justicia de la República, Dirección General de Administración, Corte Superior de Justicia de Puno, Corte Superior de Justicia de Ica, Consejo Ejecutivo del Poder Judicial y Corte Superior de Justicia de Lima.

A mis colegas y amigos de los **Formadores de Formadores de ETI PENAL**,

A mis colegas y amigos de los **Formadores de Formadores de Ciber Crimen**.

A mis colegas con quienes compartí estos años la impartición de justicia en la Corte Superior de Justicia de Lima, Susana Castañeda Otsu, Saul Peña Farfan, Miluska Cano López, Luz Victoria Sánchez Espinoza, Cesar Augusto De Vásquez y Arana de Sandoval y Covarrubias, Víctor Joe Manuel Enríquez Sumerinde, Aissa Mendoza Retamozo, María de los Ángeles Álvarez Camacho, Segismundo León Velasco, Lisdey Magaly Bueno Flores.

A los señores Jair Benavides Lanchipa, Roberto Paredes Delgado y Gustavo Alzamora Alata, Guillermo Alexander Aliaga Laberiano, compañeros entre otros dignos trabajadores de la Segunda y Séptima Sala Penal de Apelaciones de la Corte Superior de Justicia de Lima.

A mis alumnos y colegas de las diversas universidades e institutos donde preste y presto servicios con el anhelo de forjar nuevas ideas en la más excelsa de las profesiones.

A Vilmer de la Cruz Paulino, por todo el apoyo prestado en forjar este trabajo que sea útil para los lectores.

Al maestro **Manuel Lázaro Pulido** · Doctor en Filosofía por la Universidad Pontificia de Salamanca, quien, desde ese claustro educativo, permite la difusión de este trabajo a través de su sello editorial mil gracias Manuel.

Atte.
Bonifacio.

A mis padres Shirley y Bonifacio quienes me dieron la vida y a la vez me dan la dicha de ser sus colegas.

A mis hermanos, Jean Pierre Humberto, Blanca Victoria, Kiara Caroline, María Belén, Kathia Ginela y Lupita.

A mis compañeros de pre grado de la facultad de Derecho de la Universidad de San Martin de Porres,

A mis colegas y profesores de la Maestría en derecho Penal de la Universidad de Medellín – Colombia,

A mis colegas del Doctorado de la facultad de Derecho de Litigación Oral - Universidad de la Barra de Abogados de México.

A los maestros y compañeros de la Maestría en ciber criminalidad de la Universidad Internacional de la Rioja del Reino de España.

A los maestros y compañeros de la escuela de posgrado de la Universidad de Piura.

A mis compañeros del Gabinete de Asesores del Ministerio de Justicia, del Congreso de la República donde he prestado servicios.

A mis alumnos de diversas universidades y centros de educación donde venimos compartiendo nuestras exigencias académicas.

Atte. Jean Paul.