LA CIBERCRIMINALIDAD

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

COLECCIÓN CIENCIAS JURÍDICAS

COLECCIÓN CIENCIAS JURÍDICAS
Serie Derecho y gobernanza de lo público

LA CIBERCRIMINALIDAD

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

BONIFACIO MENESES GONZÁLES

JEAN PAUL MENESES OCHOA

Prologo por Sr. Dr. Antonio del Moral
Magistrado del Supremo Tribunal de Justicia del Reino de España.

Prefacio por Sr. 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

Presentación por Sr. Dr. Gustavo Jalkh Roben
Presidente del Instituto Iberoamericano de Justicia.
Ex – presidente del Consejo de la Judicatura del Ecuador.

UPSA EDICIONES
UNIVERSIDAD PONTIFICIA DE SALAMANCA

SALAMANCA
2024

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.

MENESES GONZALEZ, Bonifacio

La cibercriminalidad : consideración criminológica, político-criminal, dogmática, procesal y coope-ración Internacional / Bonifacio Meneses Gonzáles, Jean Paul Meneses Ochoa; prólogo por Antonio del Moral; prefacio por. Cristos Velasco San Martín; presentación por. Gustavo Jalkh Roben –- Salamanca: UPSA Ediciones, 2024.

613 p. ; 21 cm. – (Colección Ciencia Social y Jurídica. Serie derecho)

DL S 180-2024 -- ISBN 978-84-17601-81-2

1. Sociedad de la información. 2. Delitos informáticos. 2. Delitos informáticos-Perú-Derecho. I. Meneses Ochoa, Jean Paul. II. Tit. II. Serie

343.72:004.73

343.72(85)(094):004.73

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.: 978-84-17601-81-2
Depósito Legal: S 180-2024

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.

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

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.
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_(informática)#:~:text=En%20informática%2C%20un%20crash%20es,a%20otras%20partes%20del%20sistema
Criptografía:	http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352003000600012#:~:text=La%20Criptografía%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/Dirección_IP#:~:text=Una%20dirección%20IP%20(del%20inglés,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

ABREVIATURAS

ADP:	Anuario de Derecho Penal. Revista de la Asociación Peruana de Derecho Penal (Lima).
ADLP:	Archivo Digital de la Legislación del Perú. Publicación del Congreso de la República, Comisión de Simplificación Legislativa. Versión 1.1 Lima 2000.
ADPCP:	Anuario de Derecho Penal y Ciencias Penales (Publicación del Consejo Superior de Investigación Jurídica del Ministerio de Justicia, Madrid).
Actualidad Penal:	Actualidad Penal. Instituto Pacífico (Lima).
AnJud.:	Anales Judiciales de la Corte Suprema de Justicia de la República (Lima).
ATC:	Auto del Tribunal Constitucional.
CADH:	Convención Americana sobre Derechos Humanos / Pacto de San José de Costa Rica (1969).
CC:	Código Civil (D. Leg. 295 de 24 de julio de 1984).
CEP 1991:	Código de Ejecución Penal (Decreto Legislativo 654 de 2 de agosto de 1991).
CE:	Comunidad Europea.
CienPe:	Ciencia Penal (Río de Janeiro).
CJMP:	Código de Justicia Militar Policial (Decreto Legislativo Nº 961 del 10 de enero de 2006).
CodiCon:	Código de Conducta para Funcionarios encargados de hacer cumplir la ley. Asamblea General ONU, Res. 34/169 de 17 de diciembre de 1979.
CoNA:	Código de los Niños y Adolescentes (Ley 27337 de 7 de agosto de 2000).
ConDePri:	Conjunto de principios para la protección de todas las personas sometidas a cualquier forma de detención o presión. Adoptado por la Asamblea General ONU. Res. 43/173 de 9 de diciembre de 1988.
CoNi:	Convención sobre los derechos del niño. Asamblea General de las Naciones Unidas, Resolución 44/25 de 20 de noviembre de 1989 (entrada en vigor: 2 de setiembre de 1990).
Const.:	Constitución Política del Perú de 1993.
CP 1863:	Código Penal peruano de 1863.
CP 1924:	Código Penal peruano de 1924.
CP 1991:	Código Penal peruano de 1991 (D. Leg. 635 de 8 de abril de 1991).

CPC:	Texto Único Ordenado del Código Procesal Civil (R. M. 010-93-JUS de 23 de abril de 1993).
CPC:	Cuadernos de Política Criminal (Madrid).
DeNi:	Declaración de los Derechos del Niño. Asamblea General de las Naciones Unidas. Resolución 1386 (XIV) de 20 de noviembre de 1959.
Dictamen CJDDHH:	Dictamen de la Comisión de Justicia y Derechos Humanos del Congreso de la República del Perú, recaído en el Proyecto de Ley del Nuevo Código Penal Nº 3491/2013-CR.LIMA 2015.
D. L./D.:	Ley Decreto Ley.
D. Leg./Dec.:	Leg. Decreto Legislativo.
DPC:	Derecho Penal y Criminología (Revista del Instituto de Ciencias Penales y Criminológicas de la Universidad del Externado de Colombia, Bogotá).
D. S.:	Decreto Supremo.
DUDH:	Declaración Universal de los Derechos Humanos, Asamblea General ONU Res. 217A (III) de 10 de diciembre de 1948.
DyP:	Derecho y Política. Revista de la Facultad de Derecho de la Universidad San Martín de Porres (Lima).
Gaceta Penal:	Gaceta Penal & Procesal Penal, información especializada para abogados y jueces. Gaceta Jurídica (Lima).
InDret Penal:	Revista para el Análisis del Derecho (España).
Núm.:	Número.
SPT:	Sala Penal Transitoria.
SPP:	Sala Penal Permanente.
STC:	Sentencia del Tribunal Constitucional.
SPJTC:	Sentencia de Pleno Jurisdiccional del Tribunal Constitucional.
TCL:	Tribunal Correccional de Lima.
TP:	Título Preliminar del Código Penal.
Trad.:	Traducción.
V. gr.:	Por ejemplo.
VJ Vox Juris.:	Revista de la Facultad de Derecho de la Universidad San Martín de Porres (Lima).
Vid.:	Véase.
Vol.:	Volumen.

PRÓLOGO

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. El 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 mantenernos 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

Con el pasar de las últimas décadas se nos ha expuesto sobre los beneficios que traería la tecnología a nuestras vidas y de la necesidad de adaptarnos a estos nuevos mecanismos tecnológicos, por cuanto existía la idea de que las formas de como ejecutábamos varias de nuestras actividades ordinarias, serian obsoletas con el venir de los años.

Solo al enfocarnos en la evolución de la informática, podemos observar que en cada década su presencia se ha convertido en cada vez más y más importante en la vida del ser humano, así como en su contribución en la cúspide de sus logros. Por lo que nos hemos visto obligados a adaptarnos a estas nuevas herramientas tecnológicas.

Como un claro ejemplo, con la utilización de los primeros avances de los ordenadores computarizados en el ámbito laboral, tuvimos que dejar de lado instrumentos como la máquina de escribir, archiveros y correos físicos. De esta forma nos adaptamos a las nuevas herramientas que nos ofrecía la tecnología, sin ser expertos en su fabricación y programación, a fin de mejorar la eficacia de nuestras actividades laborales.

Asimismo, con la masificación y democratización del internet, esto ha causado diversos cambios en nuestras vidas. Con el pasar de los años, desde la llegada del internet, hemos presenciado la modificación de nuestras acciones en varios ámbitos nuestras vidas. El internet, conocida como la red de redes, ha afectado la forma de comunicarnos, acceder a información, estudiar, trabajar, nuestras actividades comerciales, así como la forma de entretenernos.

Es así que, con los avances de los ordenadores computarizados y el internet, empezamos a familiarizarnos con el concepto de ciberespacio, entendiéndolo como un nuevo lugar, no físico, en el cual podríamos acceder y realizar actividades ordinarias, así como nuevas, sin la necesidad de trasladarnos a otro espacio físico. Por lo que desde hace años se vislumbraba una nueva era donde estas tecnologías se convierten en herramientas esenciales y facilitadoras en la existencia de la vida humana. En la actualidad es innegable los beneficios de los ordenadores computarizados y su implicancia en los ámbitos sociales, culturales y económicos.

Sin embargo, a diferencia de los beneficios brindados por las nuevas tecnologías, desde sus inicios, la difusión de los riesgos que estas nuevas herramientas puedan originar, ha sido poca o casi nula. Lo cual podría tener explicación,

debido a la novedad de estos instrumentos, su aparición ha sido tan reciente que no hemos podido entender todas sus posibilidades en su totalidad. De este modo, era de esperarse, así como la sociedad se adapta a los avances tecnológicos, también lo hace la criminalidad.

En esta línea, se tiene registro que, en el año 1834, se realizó en Francia el primer ataque por medios informáticos de la historia, la cual consistió en la manipulación de un sistema de telégrafo con la finalidad de hurtar información del círculo financiero a fin de obtener de ventajas económicas.

Posteriormente, en el año 1981, en los Estados Unidos de América, por primera vez se detuvo, juzgó y condenó a una persona por la comisión de un delito informático. Nos referimos a Ian Murphy, quien era conocido como Capitán ZAP, y se le atribuyó ingresar sin autorización, mediante la utilización de medios informáticos, a los sistemas a la empresa AT&T, a fin de modificar el horario del reloj interno de la empresa, con la finalidad de obtener beneficios económicos, por medio del uso de tarifas de telefonía más baratas que las que correspondían.

Con el transcurso de los años los crímenes por medio de la utilización de medios informáticos han ido evolucionando, causando agravios a nivel mundial, en menores y mayores cantidades, tanto como patrimoniales y no patrimoniales. Asimismo, no hay una denominación exacta frente a este tipo de delitos, por cuanto ya no se habla de delitos cometidos por medios informáticos, sino de delitos ejecutados en el ciberespacio. En tal sentido se utiliza el término ciberdelincuencia o cibercrímenes, el cual tiene su origen en el idioma inglés, en la palabra *cybercrime*.

De igual forma, también se atribuye al proceso de globalización, la evolución y desarrollo de la ciberdelincuencia o cibercrimen, por cuanto este ha conllevado a nuevas formas de relacionarnos en el ámbito social, económico, cultural y político. De igual forma, la criminalidad también ha sabido adaptarse al proceso de globalización, generando nuevos riesgos los cuales debe ser atendidos urgentemente por los Estados.

La atención de estas nuevas formas de criminalidad resulta importante por cuanto, se estima que, a nivel mundial las pérdidas económicas por ciberataques, pueden alcanzar un trillón de dólares.

Al respecto, la comunidad internacional no ha sido indiferente frente a la lucha contra la ciberdelincuencia, por lo que, como primer hito importante se tiene el Convenio de Budapest, también conocido como Convenio sobre la Ciberdelincuencia. El referido convenio fue adoptado en la Sesión N° 109 del

Comité de ministros de Consejo de Europa, el 8 de noviembre de 2001, teniendo como objetivo principal la consolidación de una política a fin de brindar protección a la comunidad internacional sobre la cibercriminalidad.

En el caso peruano, mediante Decreto Supremo N° 010-2019-RE del 10 de marzo del 2019, el gobierno peruano recién ratificó el Convenio sobre la Ciberdelincuencia, estableciéndose su vigencia en el referido año. Sobre este punto, podemos tener una visión de la postura del Perú, frente al tratamiento de la ciberdelincuencia. Debido a que, a pesar de existir el mencionado convenio desde el 2001, nuestro país recién lo ratifica 18 años después, lo cual puede ser considerado preocupante en distintos niveles frente a la lucha contra la ciberdelincuencia.

Por su parte, la OEA, considera que la cantidad de cibercrímenes registrados consta de la mitad de todos los delitos contra la propiedad cometidos a nivel mundial. Asimismo, se indica que los ataques cibernéticos podrían sobrepasar el 1% del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6% del PIB.

En la XLIV Asamblea General de la OEA realizada en el año 2014, se emite el informe denominado "Tendencias de Seguridad Cibernética en América Latina y el Caribe", en el cual se advierte que en América Latina y el Caribe existe una creciente comisión de ciberdelitos, por lo tanto, es necesario su atención urgente por los gobiernos de los Estados Miembros.

Por otro lado, los ataques provenientes de la ciberdelincuencia vienen cometiéndose en el Perú desde hace años. Respecto a la Policía Nacional del Perú, conforme a los datos de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), en el periodo de octubre 2013 a diciembre de 2020, registró 12 169 delitos vinculados a la Ley N° 30096 (Ley de Delitos Informáticos). El 78% (9 515) de los delitos registrados es por fraude informático, seguido por el delito de suplantación de identidad (13%) y delitos contra datos y sistemas informáticos (6%). El delito con mayor cantidad de registros, dentro del fraude informático, corresponde a las operaciones y transferencia electrónicas y/o de fondos no autorizados, con el 86% (8 142).

Asimismo, la información proporcionada por la Oficina de Racionalización y Estadística del Ministerio Público, respecto a las denuncias por delitos informáticos (Ley N° 30096), registradas en el Sistema de Gestión Fiscal (SGF) y el Sistema Integrado de Apoyo al Trabajo Fiscal (SIATF), desde el 22 de octubre de 2013 al 31 de julio de 2020. De este modo, en el 2014 se registraron 540 denuncias y en el 2015 éstas llegaron a 907. En el 2016 se elevaron a 1410 y un

año después se duplicaron hasta alcanzar las 2 841 denuncias. En el 2018, las denuncias continuaron ascendiendo hasta llegar a 4 648, en el 2019 con 8 504 denuncias.

Por otra parte, según los datos del Poder Judicial, en los últimos 5 años solamente se ha conseguido condenar por delitos informáticos a un total de 397 personas en el Perú.

Lo referido es preocupante por cuanto no corresponde la cantidad de sentencias condenatorias en comparación a los datos recogidos de la DIVINDAT y del Ministerio Público respecto a las cifras registrados de delitos informáticos.

Aunado a ello, la pandemia mundial ocasionada por el COVID 19, nos obligó a depender en su mayoría de elementos informáticos y aparatos digitales a fin de poder continuar con nuestras labores diarias. Lamentablemente, se tiene registros que en pandemia los ciberataques han aumentado en un 400% a nivel mundial. En el caso peruano, existió la vulneración de la plataforma del Bono Familiar Universal (YANAPAY), el cual tenía como fin brindar apoyo económico para las personas más humildes afectadas por la pandemia. Sin embargo, esta plata plataforma fue vulnerada por hackers causando un perjuicio aproximado de un millón de soles.

Debemos mencionar que las autoridades peruanas han implementado mecanismos y políticas a fin de combatir la cibercriminalidad. La Policía Nacional del Perú – PNP, en el año 2005, implementó la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), la cual tiene el objetico de investigar, denunciar y combatir el crimen organizado transnacional, así como otros hechos trascendentes a nivel nacional en el campo de los Delitos Contra la Libertad, el Patrimonio, la Seguridad Pública, la Tranquilidad Pública, la Defensa y Seguridad Nacional, la Propiedad Industrial y otros, que se cometan mediante el uso de la tecnología de información y comunicación, capturando los indicios, evidencias y pruebas, e identificando, ubicando y deteniendo a los autores, con la finalidad de ponerlos a disposición de la autoridad competente.

Posteriormente, en el año 2013, se publica la Ley N° 30096 – Ley de Delitos Informáticos, con el objeto de prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos de información y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

Por su parte, el Ministerio Público, en el año 2021 inaugura la primera Unidad Fiscal Especializada en Ciberdelincuencia con competencia nacional, teniendo como objetivos específicos efectuar la orientación técnico-jurídica en las investigaciones de los delitos cometidos por medios tecnológicos, desde la identificación y preservación de la evidencia digital.

Los referidos esfuerzos han sido importantes en la lucha contra la cibercriminalidad en el Perú, no obstante, estos no han sido suficientes. Si observamos las acciones implementadas por los países de la región, como Chile, Ecuador, Colombia y Argentina, podemos advertir que han implementados políticas de ciberseguridad destinadas a brindar seguridad de las personas en el ciberespacio. Sin embargo, el Perú, no tiene políticas en ciberseguridad a fin de buscar protección de los peruanos frente a los ciberataques.

Conforme a lo expuesto, existe la necesidad por parte del Perú en brindar políticas en ciberseguridad, de igual forma, en la actualidad, nuestra legislación no prevé una ley en ciberseguridad.

Al respecto, podemos advertir que en el Perú no terminamos por entender la magnitud de la no prevención y el poco tratamiento de la ciberdelincuencia. En otros países ya se considera al ciberespacio como un dominio de guerra o de combate, al igual que los clásicos como: tierra, mar, aire y espacio.

Vivimos en una época donde nuestras actividades dependen de medios informáticos y tecnológicos. Dependemos de estas herramientas al ejecutar nuestras labores profesionales, en la forma de hacer comercio, en nuestros estudios y hasta la forma de entretenernos. Las redes sociales representan una carta de presentación frente a lo que conocemos como la sociedad de la información. Nos comunicarnos con varias personas en forma inmediata pueden encontrarse en diferentes lugares del mundo. Podemos realizar compras en línea por medio de nuestros celulares sin la necesidad de interactuar con seres humanos y sin salir de nuestros hogares.

En el campo judicial ahora podemos participar en audiencias virtuales por medio de software de video conferencias, las cuales se ha visto comprometidas mediante intrusiones no autorizadas de usuarios desconocidos. Aquí podemos mencionar un ejemple de la vulnerabilidad de las audiencias virtuales, por cuanto que, hasta en una audiencia en la que se estaba inmerso, en calidad de investigado, el presidente de la República, Pedro Castillo Terrones, sufrió la intrusión de un usuario desconocido el cual pudo proyectar un video de un conocido bailarín, menguado la seriedad de la audiencia virtual y el tiempo de los que

formaban parte de la referida audiencia. En tal sentido, no podemos brindar seguridad a la audiencia virtual del más alto dignatario del País.

Para entender el nivel de vulnerabilidad a la que estamos expuestos a riesgos por la cibercriminalidad, solo debemos revisar los datos sobre la cantidad de personas que tienen algún vínculo con el ciberespacio.

En tal sentido, se tiene que, en el Perú, en los primeros tres meses del 2022, 73 de cada 100 personas de 6 y más años de edad accedieron a Internet en el país, cifra que muestra un crecimiento de 5,1 y 17,7 puntos porcentuales al compararla con igual trimestre de los años 2021 (67,4%) y 2019 (54,8%), respectivamente. Así lo dio a conocer el Instituto Nacional de Estadística e Informática (INEI) a través del informe técnico Estadísticas de las Tecnologías de la Información y Comunicación en los Hogares, elaborado con los resultados de la Encuesta Nacional de Hogares (ENAHO)[2].

Además, respecto al uso de celulares en el Perú, se tiene registro que en el 68,8% de los hogares los miembros tienen únicamente teléfono celular, lo cual aumentó en 2,9 puntos porcentuales en comparación con similar trimestre del año pasado; en el 21,8% de los hogares los residentes tienen celular y además teléfono fijo y el 1,3% tienen únicamente teléfono fijo. Por último, el 8,0% de los hogares del país no cuenta con ningún tipo de telefonía[3].

Respecto al uso de redes sociales, se tiene que el total del número de usuarios en las redes sociales es de 27 millones de peruanos. Esto equivale al 81,4% de la población total. A su vez, el porcentaje de usuarios en redes sociales es del 81.4%. Con respecto al año 2020 hubo un incremento del 12,5% con 3 millones de nuevos usuarios. En Perú 26.41 millones de usuarios acceden a las redes sociales a través de teléfonos móviles lo que representa 97,8%[4].

En atención a lo expuesto, podemos observar la cantidad de personas vinculadas al ciberespacio, lo cual crea nuevas áreas de vulnerabilidad, las cuales

---

[2] Nota de Prensa (s.f.) El 72,5% de la población de 6 y más años de edad del país accedió a Internet en el primer trimestre de 2022. Instituto Nacional de Estadística e Informática – INEI. Recuperado el 18 de septiembre de 2022. De: https://m.inei.gob.pe/prensa/noticias/el-725-de-la-poblacion-de-6-y-mas-anos-de-edad-del-pais-accedio-a-internet-en-el-primer-trimestre-de-2022-13767/#:~:text=En%20los%20primeros%20tres%20meses,54%2C8%25)%2C%20respectivamente.

[3] Nota de Prensa. (s.f.). En el 90,6% de los hogares del país existe al menos un miembro que tiene teléfono celular. Instituto Nacional de Estadística e Informática – INEI. Recuperado el 18 de septiembre de 2022. De: https://m.inei.gob.pe/prensa/noticias/en-el-906-de-los-hogares-del-pais-existe-al-menos-un-miembro-que-tiene-telefono-celular-10412/

[4] Alvino, C. (07 de mayo de 2021). Estadísticas de la situación digital de Perú en el 2020-2021. Branch. Recuperado el 18 de septiembre de 2022 de: https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-peru-en-el-2020-2021/

pueden y son aprovechados para cometer cibercrímenes o ciberataques. Lo referido resulta importante puesto que, debido a la masificación de los smartphones, en la actualidad es común realizar transacciones bancarias y comercio por medio de estos dispositivos, lo cual abre un espacio para grandes pérdidas patrimoniales.

En relación a ello, no solo la ciudadanía esta expuestos a los ciberataques, por cuanto sitios web de diferentes entidades pública del Perú ha sido vulneradas. Tenemos el caso del portal web de la presidencia de la república, el portal web del Tribunal Constitucional, el portal web de la Policía Nacional del Perú. Las entidades privadas no han sido ajenas a estos ataques, lamentablemente varias entidades bancarias y empresas del Perú también han sido víctimas en el ciberespacio.

De este modo, el Estado Peruano, a través de sus órganos y organismo públicos deben implementar acciones inmediatas de corto y largo plazo, con la finalidad de evitar los ataques por parte de la cibercriminalidad y evitar que el ciberespacio en el Perú se convierta en lo que se conoce como un paraíso para la impunidad.

Resulta complicado intentar precisar qué es lo que pasará en un futuro cercano y lejano, en la situación por no implementar medidas de protección contra la cibercriminalidad y ciberseguridad. Es un hecho que las tecnologías irán evolucionando y perfeccionando los fines para los cuales fueron creados. También es un hecho que nuestras vidas dependerán cada vez más de estas tecnologías.

Podemos utilizar obras de la literatura y del cine relacionados a la ciencia ficción para hacernos ideas, que en muchos casos han acertado en su visión del futuro, como es el caso de la película Odisea en el espacio, dirigida por Stanley Kubrick y estrenada en 1968. El referido largometraje presentó tecnologías las cuales recién aparecieron en décadas posteriores, como videollamadas por medio de dispositivos, tablets portátiles e inteligencia artificial.

Actualmente existen varias películas las cuales nos pueden dar una idea de lo que nos estaremos enfrentando en las próximas décadas, las cuales muchas han precedido o sean acercado mucho a nuestra realidad actual.

Desde la literatura tenemos obras como Neuromante, del canadiense William Gibson, publicada en 1984, en la cual aporta a la tecnología, términos como Ciberespacio. Asimismo, no podemos dejar de referirnos la novela del británico conocido por el seudónimo de George Orwell, titulada 1984, en la cual se relata una distopía, donde los ciudadanos se encuentran vigilados y controlados por el

aparato de poder conocido como el Gran Hermano, en una sociedad totalitaria e hiperpolitizada. En la actualidad, muchos opinólogos indican que vivimos en una sociedad como la expuesta en la obra 1984, esto debido a nuestra vinculación con los aparatos tecnológicos y redes sociales.

En atención a lo expuesto, podemos advertir la importancia y necesidad del Estado peruano, por medio de sus instituciones públicas que conforman el Sistema Penal, en implementar medidas, políticas y reformas legales a fin de combatir y prevenir los ataques por medio de la cibercriminalidad o ciberdelincuencia. Al no existir una política que proteja a la sociedad en el uso de las tecnologías de la información y comunicaciones, esto pone en riesgo los derechos de las personas, así como de las empresas privadas y las instituciones públicas.

Por tales motivos, surge la justificación de la presente obra, por cuanto creemos que, para brindar un tratamiento óptimo en la lucha contra la cibercriminalidad, debe existir un Sistema Penal preparado e idóneo para tales fines. De este modo, en esta obra presentamos un estudio sobre desde la Política Criminal, Criminología, Derecho Penal, Derecho Procesal, aplicados en al Sistema Penal en su tratamiento de la cibercriminalidad.

Desde la academia pretendemos presentar propuestas con la finalidad de mejorar la lucha contra la cibercriminalidad, dirigido a quienes forman parte del sistema penal, nos referimos a los defensores, policías, fiscales y jueces. Asimismo, este libro también está dirigido a los que tengan como fin el estudio de la cibercriminalidad.

Aunado a ello, la presente investigación también ofrece propuestas legales a fin de mejorar la investigación y procesamiento de la cibercriminalidad, por lo que también está dirigido para funcionarios del Poder Legislativo.

En tal sentido, en el primer capítulo desarrollamos conceptos relacionados a la informática, el internet, el ciberespacio y sociedad de la información. Esto es importante para la presente obra, por cuanto es necesario conocer los conceptos básicos en donde se desarrolla la cibercriminalidad. Para el estudio de la cibercriminalidad, resulta necesario conocer la sociedad en la cual nos desenvolvemos.

En el segundo capítulo expondremos la problemática sobre la cibercriminalidad en el sistema de justicia, para eso revisaremos los datos y estadísticas brindadas por la Policía Nacional del Perú, Ministerio de Justicia y Derechos Humanos, Ministerio Público – Fiscalía de la Nación, Defensoría del Pueblo y el Poder Judicial. Además, revisaremos informes elaborados por entidades

internacionales, a fin de entender como el sistema de justicia peruano atiende a esta nueva forma de criminalidad con nuevas tecnologías.

En el tercer capítulo desarrollaremos los conceptos de ciberseguridad, ciberdefensa y protección de datos personales. Los referidos conceptos resultan sustanciales para la presente investigación, esto debido a que, para garantizar la lucha contra la ciberdelincuencia como políticas públicas, es necesario saber de ciberseguridad. De igual forma, se realizará un estudio comparado de la ciberseguridad y ciberdefensa en otros países.

El cuarto capítulo está enfocado en los aspectos criminológicos de la cibercriminalidad, el ciberespacio como plataforma delictiva, sus factores y caracteres, el ciberdelincuente y la cibervíctima.

En el quinto capítulo se abordará el tema de las consideraciones dogmáticas de la cibercriminalidad, luego, en el capítulo sexto se desarrollarán las conductas punibles en la legislación nacional.

En el capítulo séptimo expondremos las posibilidades de aplicar los procedimientos especiales en los delitos informáticos con la finalidad de contribuir eficientemente a la lucha contra la cibercriminalidad.

En el capítulo octavo desarrollaremos el tema de los órganos jurisdiccionales especializados en cibercriminalidad, a fin de demostrar la necesidad de su implementación y su factibilidad de esta con la finalidad de mejorar el procesamiento de los delitos informáticos en el Perú.

En el capítulo noveno trataremos el tema de la prueba en el proceso penal de los ciberdelitos, el cual resulta importante su tratamiento por cuanto su aplicación en el proceso relacionado a los cibercrímenes requiere un tratamiento especializado.

En el capítulo décimo trataremos la cooperación internacional en la cibercriminalidad y en el capítulo décimo se desarrollará el tema de los cripto activos y criptomonedas.

Es necesario conocer la jurisprudencia que se ha expedido en algunos casos, que si bien es cierto no es profusa en el Pais, nos lleva a entender para el lector que ribetes de análisis tienes nuestros jueces en ese extremo para conocer la ciberdelincuencia, además que en el capítulo final tenemos los instrumentos necesarios que podamos tener de consulta inmediata sobre El Convenio de Budapest y el protocolo adicional necesario para ver el perfil futuro de la lucha global contra esta pandemia y finalmente una dedicada bibliografía que igualmente debe ser de entera utilidad para los lectores.

Es preciso señalar el interés de los autores en el conocimiento, entendimiento y difusión de tan delicado tema como es el embate del ciber crimen y la exposición y desprotección de los ciudadanos frente a una nueva pandemia que es la comisión de estos delitos que van más allá de la simple comisión del evento, va atentar en su momento con la propia estructura del sistema democrático y será con tristeza un escenario delictual, de lavado de activos, pornografía infantil, delitos contra la administración pública, delitos contra el honor, contra el patrimonio y la secuela sistemática de figuras que aparezcan por su condición de pluriofensividad, además del grave perjuicio que la ciudadanía, más el Estado se verá gravemente perjudicados.

En atención a lo expuesto, coincidimos con Emily Durkheim, cuando señala que "*la criminalidad es un flagelo normal en aquellas sociedades que alcanzan mayor desarrollo y complejidad*"[5]

Si bien es cierto el estudio programático de los delitos informáticos desde su aparición en el Código Penal del año 1991, su repercusión del desarrollo de la tecnología en todos los sectores de la vida humana, como profesor de Universidades del País, como del extranjero tuvimos a bien incidir en esta nueva modalidad delictiva, siendo una materia de estudio y enseñanza, sin embargo, debido al avance de la tecnología y la exposición de las redes sociales, esta figura delictiva tuvo mayores consideraciones de asistencia dogmática como de difusión jurídica y preocupación mundial, teniendo por tanto la realización de eventos más continuos del tema en ámbitos universitarios.

La preocupación por este capítulo del derecho penal, se inicia en los estudios de pos grado ante la Universite Droit del Homme en Ginebra – Suiza, donde profesores de estirpe mundial ya nos alarmaban de lo que pasaría en el futuro del derecho penal, con el advenimiento de la tecnología y el uso de criminales que usarían la misma con fines execrables como lo vemos ahora, algo así como Alvin Toffler en su "tercera ola" o "el shock del futuro", asimismo, debo precisar que respecto al aspecto procesal sobre esta figura delictiva, lo discutimos en los estudios en la "Western School of Law" de San Diego California, con preocupación absoluta de la forma como se tendría que batallar en temas de aplicación espacial de la ley penal o el interrogatorio frente a testigos hostiles o que no colaboren para el mejor esclarecimiento de los hechos.

Sin embargo, el estudio de envergadura y exigencia sobre el tema, cobra fuerza al ser becado a ILEA – Roswell EEUU, "La Academia Internacional para

[5] Revue Philosophique, 20, XXXIX, enero a junio de 1895, pp. 148-162. Traducción al castellano de Alina Ríos (Universidad de Buenos Aires).

el Cumplimiento de la Ley" (ILEA) de Roswell, Nuevo México; es la academia de capacitación avanzada para profesionales de orden público internacionales del Departamento de Estado de los Estados Unidos. ILEA Roswell, que ofrece instrucción académica de nivel superior sobre las últimas técnicas de orden público y justicia penal al proporcionar a los oficiales de orden público extranjeros habilidades y conocimiento para investigar y combatir delitos de forma eficaz en sus respectivos países. Teniendo el honor de asistir representando al Perú por aproximadamente 31 días, conjuntamente con 5 integrantes de la Policía Nacional de Perú, Marco Lara Vergara, Miguel Cayetano Cuadros, Rubén Yáñez Castañeda, Carlos Suarez Garrido y Carlos Diaz Apolinario(+); 5 señores fiscales del Ministerio Público, Fanny Quispe Farfán, Edgar Espinoza Casas, Tanya Bravo Vigo, Mirko Cano Gamero, y Pedro Washington Luza Chullo, 5 Jueces, donde destacaron: la Dra. Susana Castañeda Otsu, Juan Riquelme Guillermo Piscoya, Segismundo León Velazco, Jorge Calderón Castillo y el co autor de la presente obra, sumado un digno representante del Ministerio de Justicia como es el Dr. Justo Balmaceda Quirós, el curso fue dictado por funcionarios de la **CIA, DEA, Servicio Secreto de los EEUU, FBI e Interpol,** siendo el tema central el advenimiento de la ciber criminalidad - Cyber Financial Crimes Strategy Executive Policy and Development Study –

El evento de polendas contó con quince representantes de Ecuador e igual número de juristas Colombianos, con la asistencia del gobernador y demás autoridades de Nuevo México – Roswell – fueron esos estudios programáticos que hicieron el llamado de atención para una vez de retorno al Perú, con todo ese bagaje de aprendizaje, empezamos a diseñar el libro que ahora presentamos y la difusión en cada distrito judicial y fiscal en el interior de la República, por ello el agradecimiento a todos los señores presidentes de las Cortes Superiores que tuvieron a bien invitarnos a sendos seminarios y congresos internacionales, a su vez, el co autor Jean Paul Meneses Ochoa, desarrolló todo el conocimiento sobre este escenario delictivo en la Universidad de Medellín - Colombia, donde obtuvo el grado académico de Magister, asimismo los estudios adyacentes en San Juan de Puerto Rico, Cartagena de Indias en Colombia y ser doctorando de la Universidad de la Barra de Abogados de México, donde concluye sus estudios para optar el grado de doctor en Derecho.

Sobre el tema esencial se fortaleciendo los estudios de ciber crimen con el aval y sustento de la Agencia Española de Cooperación Internacional -AECI- en sus sedes de Cartagena de Indias, Montevideo, Santa Cruz de la Sierra y Antigua Guatemala, lugares que gracias a la conducción de la distinguida maestra y mejor amiga **Rosa María Tome García**, de la Audiencia Nacional del Reino de

España, como encargada en el Ministerio de Justicia para tamaña responsabilidad, demostrando el éxito total en cada jornada donde conocimos a colegas de toda Iberoamérica con el peculiar estilo de enseñanza, como de mejor conocimiento del tema, luego ella, tuvo la bondad de acudir a nuestro llamado en Lima para capacitar a jueces y fiscales en temas de su especialidad, gracias a esos eventos llevados a cabo en los últimos siete años, junto a Roswell, fuimos invitados a España, para participar y discutir sobre el espacio que generaba en el mundo el ciber crimen, teniendo el privilegio de ser expositor en sendos eventos como el El CURSO SUPERIOR EN DERECHO EN CIBERDELITOS es un Programa de Formación, con titulación de reconocimiento internacional, dictado y certificado por la Fundación General de la Universidad de Salamanca (España), y avalado por la Comunidad Europea, en las instalaciones del Ilustre Colegio de Abogados de Granada.

A su vez, estos eventos nos abrieron las puertas de las jornadas anuales **"Román García Valera"**, grata invitación del señor alcalde del Ayuntamiento de Sarria, D. Claudio Garrido Martínez, celebradas en la Villa de Sarria, Xunta de Galicia**,** evento que ha cobrado vigencia absoluta en su realización cada año, con la presencia y repercusión de toda la Península Ibérica, estas jornadas, son un encuentro que tuvo su origen en el año 2007. Tras el fallecimiento de su fundador en 2013 han proseguido su celebración en memoria del Magistrado hasta la actualidad. El foro tiene lugar en la localidad de Sarria (Lugo) por la que transcurre el camino de Santiago. Todos los años acuden prestigiosos ponentes, tanto nacionales como internacionales, que debaten sobre temas de gran interés y trascendencia jurídica.

Por ello reitero y suscribo haber conocido a dilectos expositores que muy preocupados por el embate del ciber crimen como por la protección de datos, me permitió conocer **al maestro y mejor Juez Antonio del Moral, Magistrado del Supremo Tribunal del Reino de España,** que ha tenido la bondad de prologar el presente trabajo con un sentimiento abrumador del amor del padre al hijo y del hijo al padre, gracias gran amigo.

Las ponencias de fuste simplemente hicieron de temas tan delicados, de difícil entendimiento, hacerlos digeribles para el conocimiento general, apreciando la presencia de la Dra. Victoria Ortega Benito presidenta del Consejo General de la Abogacía, Dr. Pascual Sala Sánchez, expresidente del Tribunal Constitucional. Dr. Joaquín Huelin Martínez de Velasco, magistrado de la Sala Tercera del Tribunal Supremo en excedencia, Dr. Antonio López Díaz, rector de la Universidad de Santiago de Compostela y catedrático de Derecho Financiero y Tributario. Dr. Juan Antonio Xiol Ríos. Ex vicepresidente del Tribunal

Constitucional, Dra. Emilia Casas Baamonde, ex presidenta del Tribunal Constitucional y catedrática de Derecho del Trabajo y Seguridad Social en la Universidad Carlos III de Madrid, Dr. José Luis Seoane Spiegelberg, magistrado de la Sala Primera del Tribunal Supremo, Dr. Luis López Guerra, ex vicepresidente del Tribunal Constitucional y ex presidente de sección del Tribunal Europeo de Derechos Humanos, Dr. Juan José González Rivas, ex presidente del Tribunal Constitucional y por supuesto mi agradecimiento a un dilecto amigo el Dr. Román García-Varela Iglesias. Director de las XVI Jornadas Jurídicas y que honra la memoria de su señor padre.

Ahora bien, debo agradecer a las escuelas judiciales de Republica Dominicana, Guatemala, Costa Rica, donde hemos discutido cada uno de los presupuestos jurídicos de ciber delincuencia, personajes además en diversos países que vienen difundiendo y explicando todos los problemas que se nos vienen presentando para enfrentar a esta nueva pandemia que viene a ser esta figura delictiva, entonces es momento de viajar por el mundo cibernético o que ponen el hombro en la capacitación y fomento del desarrollo de los jueces y fiscales en fortalecer las virtudes que hacen posible la consagración de tal formación académica; por ello felicitar y agradecer a diversos personajes de la judicatura mundial, es el caso de Colombia y por ello mi reconocimiento al maestro y Fiscal en Jefe de Medellín, Mario Nicolas Cadavid Botero, privilegio mayor que conservamos de haber sido profesor nuestro en la Universidad de Medellín, a la fiscal encargada de la lucha contra la corrupción Luz Adriana Londoño Bonilla, con quien compartimos innumerables jornadas académicas en muchos países de Latinoamérica, al Sr. Dr. David Gutiérrez Castaño por su compromiso docente, Director de la Unidad de Pos Grado de la Universidad de Medellín, destacado conferencista que ha recorrido todo el Perú apoyándonos en capacitar abogados, jueces y fiscales, quienes siempre lo recuerdan como el mayor cariño, a la señora Decana de la facultad de derecho y Ciencias Forenses de la Universidad Politécnico de Antioquia Luz Elena Mira Olano, felicitaciones por su labor y agradecidos por siempre aprender de sus enseñanzas y su excelente humor, sin olvidarme de Carlos Jaramillo mejor criminalístico que pude conocer y el destacado abogado Juan Mario Cadavid, dilectos personajes del foro colombiano. Asimismo, a los profesores Juan Camilo Muñetón Villegas y Federico Londoño Mesa por sus importantes enseñanzas en el derecho penal y procesal penal.

No podemos dejar de agradecer a aquellas personas que han hecho posible la edición de este trabajo, juristas de cada país que hemos tenido el honor de compartir el podio en diversos certámenes de esta figura delictiva que causa infinidad de problemas a la colectividad mundial, por ejemplo en republicas

hermanas donde fuimos recibidos con afecto imperecedero, Ecuador, el Maestro **Gustavo Jalkh Roben** ex presidente del Consejo de la Judicatura de ese hermoso país, destacado expositor y mejor amigo, quien conjuntamente con los dignos integrantes de la Asamblea, nos han permitido integrar **"El Instituto Iberoamericano de Justicia"** con diversas sedes desde España hasta nuestra región, es actual Presidente del IIBJ, donde destaca entre otros el gran jurista Tomas Alvear Peña, y tiene como dignos integrantes a Ramiro Rivadeneira Silva, Nestor Arbildo Chica, Tomas Montero Hernanz.

Debemos señalar, que la publicación de estas letras se debe en gran medida al apoyo del maestro y mejor amigo **Manuel Lázaro Pulido** · Doctor en Filosofía por la Universidad Pontificia de Salamanca, quien desde ese claustro educativo, permite la difusión de este trabajo y hará posible que llegue a sus manos para mejor entender y comprender el ciber delito.

Nuestro agradecimiento eterno al juez de jueces Julio Aguayo Urgiles, su brillante trayectoria de Guayaquil, institucionalista y forjador de las Unidades de Flagrancia del Ecuador, que abusando de su fe en la enseñanza del derecho acudió las veces que fue convocado a nuestro país y recorrio palmo a palmo cada recondito lugar para capacitarnos, además, jueces ecuatorianos, como Daniela Mayorga, Paulina Zarsoza que hacen de la justicia en su tierra un don inacabable de aceptación general. Sin olvidar las enseñanzas de un joven abogado y mejor docente Diego Camacho.

Siempre que hablamos sobre la cibercriminalidad, debemos señalar que en Chile le dieron un tratamiento serio, desde la formación de su personal y el soporte técnico en el estudio y aplicación de la cibernética e inteligencia artificial para el uso de la justicia y todo un sistema encargado del correcto desarrollo institucional para ese efecto, en concreto el gurú de ese logro en Chile, es el ingeniero **Mario Lara Orellana**, que a nivel de la Corte Suprema y en cada región del vecino país implementaron para mejor auspicio el expediente electrónico y el soporte técnico para la justicia, desde que nos conocemos participamos en innumerables eventos académicos, de quien no dejo de aprender, tanto así, su destacada participación en el "Octopus 2023" La Conferencia sobre cooperación en materia de ciberdelincuencia y pruebas electrónicas se celebró del 13 al 15 de diciembre de 2023 en Bucarest, Rumania, La Conferencia Octopus es parte de la iniciativa del Consejo de Europa. Se basa en contribuciones voluntarias para ayudar a la implementación del Convenio de Budapest sobre Ciberdelincuencia y abordar los desafíos emergentes a partir de 2020. La conferencia reúne a expertos en ciberdelincuencia de más de 100 países, organizaciones internacionales, el sector privado y el mundo académico para intercambiar sus

puntos de vista y conocimientos sobre la ciberdelincuencia. Este año la atención se centrará en proteger y compartir pruebas electrónicas y desarrollar capacidades en materia de delitos cibernéticos y pruebas electrónicas

Sigo en Chile y mi reconocimiento al ex presidente de la Corte Suprema, **Guillermo Enrique Silva Gundelach,** quien le impuso celeridad y desarrollo a todo ese sistema muy respetado en el mundo entero de la justicia moderna en Chile, tuvimos el privilegio de compartir innumerables veces temas de este y muchos problemas de la judicatura regional, allá en las aulas de la Agencia Española de Cooperación Internacional -AECID- con sede en Antigua Guatemala, gracias Willy, igual reconocimiento a dilectos juristas chilenos como Ricardo Tucas, Rodrigo Orellana, además de los preclaros fiscales Julio Contardo y Patricio Caroca, con todos ellos hicimos la promesa de difundir y trabajar este hito de la historia penal internacional la lucha contra la ciber delincuencia.

Si viajamos a Argentina, no dejamos de felicitar y agradecer a los compañeros de la Facultad de Derecho de la UBA Universidad de Buenos Aires que en la actualidad vienen siendo el faro regional en el estudio programático de la ciber delincuencia o su aporte definitivo a la mejor forma de impartir justicia como Julio Corvalán, en su afamado y gran proyecto de justicia. PROMETEA, que el mundo entero tiene que hablar de dicho gran proyecto, amigos del foro Argentino entre maestros, jueces y mejores juristas que siempre estamos en contacto y hablamos de estos temas, como José Antonio Michelini, nuestro profesor en la Universite Droits del Homme – Ginebra – Suiza, Carlos Vera Barros, colega y mejor juez entrañable amigo, Juan Carlos Carretero otro jurista de época, Decano de la facultad de las Flores, Claudio Santagatti, vicepresidente de la Asociación de Magistrados de Argentina, quien me acompañó en sendas actividades académicas desde muchos años, Ana Clara Manasero, Julio Mayer que nos ilumina desde donde lo tenga Dios, Héctor Nieri, Alberto Binder López, German Bidart Campos, Antonio Puccineli, con quien tuve el honor de compartir podio en el III Congreso Latinoamericano de Derecho en la bella ciudad de Cochabamba en Bolivia. A todos ellos siempre agradecido por sus enseñanzas y capítulo aparte a un gran jurista, amigo del alma, que tuvo la bondad de invitarme a su incorporación como juez de la Corte Interamericana de Justicia en San José de Costa Rica al maestro Eugenio Raúl Zaffaroni, asimismo, en la época que iniciamos con especial énfasis los temas de la victimología, participamos en el primer congreso Mundial en la Habana Cuba, donde conocí al destacado jurista Elías Neuman, que en tiempos anteriores hablaba del "Sida en las Cárceles" como escenario de genocidio, en ese memorable evento se encontraban además otros destacadísimos expositores y de ahí se forjo amistades, como Ezza Fatah,

Emilio Viano, el maestro Luis Rodríguez Manzanera y su distinguida esposa María de la Luz Lima Malvido, quienes han hablado y escrito tanto sobre la víctima del delito; espero no olvidarme de algún amigo que la vida nos regaló.

Costa Rica, siempre y será un lugar donde nacen juristas, se desarrollan y exportan como la propia CIDH fallos que regulan la vida jurídica de América, por ello mi recuerdo y respeto de siempre al incansable jurista, 16 años presidente de la Corte Suprema de Justicia, Ministro de Justicia, hombre de bien, que nos dejó muy joven y tenía mucho más que producir, nuestro homenaje a Luis Paulino Mora Mora, quien zanjó la idea del cambio en la justicia latinoamericana, propulsor de los tribunales de flagrancia y hoy por hoy, sigue siendo un ejemplo de justicia, tuvo la gentileza de acudir a mi asunción como Presidente de la Corte Superior de Justicia de Ica, el cielo tiene una estrella más que admirar, ese legado nos permitió conocer a otros grandes personajes de la justicia costarricense, como Alfredo Araya Vega, quien ha venido a nuestro país, las veces que le ha sido posible a capacitar en el tema del proceso inmediato y expositor ante los jueces supremos en el Pleno Jurisdiccional 2-2016, junto a él reconozco a Carlos Núñez Núñez, juez de flagrancia que igualmente acudió a nuestro llamado para compartir actividades de capacitación a nivel nacional, Carlos Morales Chinchilla, Juez Supremo, Randal Moya Valverde, Juez de Flagrancia de San José, entre otras grandes maestros.

Debemos seguir en ese viaje interminable de juristas que han aportado para escribir este libro, es el caso de llegar a Panamá y señalar a un distinguido Juez que ahora forjamos una amistad imperecedera, Gustavo Romero-Duque, con quien a diario compartimos conocimientos de derecho, asimismo la Dra. Jannette Diaz, destacada jurisconsulta panameña, además que fuera representante de la belleza de su país a un concurso mundial como Miss Universo, ellos se suman a otros distinguidos colegas del foro panameño, cerca de tan importante país, en República Dominicana, agradezco a la Escuela Nacional de la Judicatura, donde tengo el honor de dictar clases y conferencias, al señor Presidente de la Corte Suprema de Justicia, Luis Henry Molina Peña, por todas esas consideraciones, con nosotros y a la Dra. Esther Elisa Agelan Casasnovas, Juez Suprema y carísima amiga, todo el apoyo brindado en sendas actividades académicas como la sugerencia en publicar estas líneas.

Hemos tenido la oportunidad de estar en Guatemala, lugar paradisiaco donde igualmente se respira el compromiso de los juristas en discutir y difundir la cultura jurídica, en tan cálido país, conocimos destacados jurisconsultos que es un privilegio tener su aporte en la redacción de este trabajo, Rafael Solares Morales, Presidente de la Junta Directiva del Instituto de Magistrados, de la

Corte de Apelaciones Organismo Judicial de Guatemala, la Dra. Claudia Marine de León Teo, presidente de la Asociación de abogados y notarios de Izabal, grandes colegas que inspiraron con sus comentarios la redacción de este trabajo, como la Dra. Karoll Vásquez, magistrada destacada e integrante del Consejo Ejecutivo del Poder Judicial, Nelly Maribel Mejicano Quiñonez, juez Penal con dedicación a su delicada labor, especial reconocimiento a la Dra. Rosmeri López Pérez, con quien hemos tenido el privilegio de compartir el podio en diversos eventos académicos en Latinoamérica, todos ellas coadyuban en el desarrollo de la justicia de tan bello país, como agradecimiento supremo al caro amigo Luis Adolfo López Oliva, representante de la Facultad de Derecho de la Barra de Abogados de México, gracias por todo ese apoyo.

Hace poco pudimos destacar el trabajo que viene desarrollando el sistema de justicia de El Salvador, pequeño país, pero de grandes hombres y mujeres de derecho, por ello es preciso destacar personalidades que nos atendieron de la mejor manera en ese pedazo de paraíso que es San Salvador, la Dra. Gerardine Aldana Revelo, Directora de la Unidad Técnica Ejecutiva de El Salvador, sabia docente y mejor Juez, de igual manera a la Dra. Carolina Monterrosa, por todo el apoyo logístico al desarrollo del evento "Inteligencia Artificial aplicada a la Justicia", nuestro recuerdo de siempre al Juez y mejor amigo William Francisco Gutiérrez Avelar, a quien conocemos desde Cartagena de Indias, muchos años atrás y las continuas capacitaciones en diversos países de habla hispana, gracias por capacitar a los jueces y fiscales del Perú y por todas las atenciones brindadas en su país.

Solo para destacar y refrendar nuestra amistad y agradecer por su invitación a nuestros amigos de la República del Paraguay, como el Juez Supremo Manuel Aguirre y el nieto del principal héroe Paraguayo José Félix Fernández Bilbao, gracias señores, de la visita a Uruguay como no destacar a Marcelo Pecse, quien tuvo el más alto cargo administrativo ejecutivo del país oriental y puso adelante un sinfín de medidas que ayudaron a su desarrollo, compartimos en Granada – España un espacio académico y se sembró una dilecta amistad.

Si llamamos nuestra segunda patria, debemos decir siempre que México nos albergó infinitas veces, desde la Asociación de Doctores en Derecho, el sueño de dictar una conferencia en la Universidad Autónoma de México, de estar con grandes maestros en el auditórium "Benito Juárez", en la Suprema Corte de Justicia, pertenecer a la plana docente de la Universidad de la Barra de Abogados de México, facultad iberoamericana de litigación oral, con distinguidos alumnos en la escuela de doctorado, lugar los autores compartimos catedra, como profesor y alumno y luego colegas en la vida académica. Por ello saludo al señor rector

Rubén Pacheco Inclan, a la directora académica, doctora Adriana Arroyo Cuevas, al motor de la facultad, Juan Manuel Guerrero Almaraz.

El recuerdo vivo de haber dictado sendas conferencias en parajes maravillosos como Zacatecas, Guanajuato, San Luis de Potosí, Puebla, Guadalajara, Estado de Guerrero, Michoacán, pero donde mayor tiempo hemos dedicado es en Morelos, Cuernavaca, paraíso terrenal de mejor clima y grandes personalidades del derecho, como es el señor presidente del Superior Tribunal de Morelos, Luis Jorge Gamboa Olea, entrañable hermano y mejor juez, quien ha recorrido el Perú entero para capacitar, jueces, fiscales y abogados en el nuevo código procesal penal, justamente en aquel memorable tiempo que tuvimos la conducción de la implementación del NCPP al Perú, desde el Consejo Ejecutivo del Poder Judicial, donde tuvimos el honor de representar a los jueces superiores de todo el país. A su vez que estuvimos en el XV Congreso Mundial de Jueces en Nueva Delhi, India y esa amistad es imperecedera con el tiempo.

Ahora bien, el Poder Judicial tuvo la decisión histórica de conformar a través del Equipo Técnico de implementación del Código Procesal Penal un especial grupo de trabajo llamado "**Formador de Formadores**" grata experiencia y nuestro reconocimiento a todos los señores magistrados que integraron tan selecto como nutrida representación a nivel nacional, siendo el magistrado Jorge Luis Salas Arenas, Juez Supremo que dirigió con absoluta sensatez, honor y conceptualizó la unidad de los formadores, cuya representación nacional se advirtió como Fanny María Andrade Gallegos, Consuelo Cecilia Aquize Diaz de Montes de Oca, Oscar Manuel Burga Zamora (+) que desde el Cielo nos protege, Víctor Alberto Martín Burgos Mariños, Juana Mercedes Caballero García, Susana Ynes Castañeda Otsu, Tony Rolando Changaray Segura, Juan Carlos Checley Soria, Nayko Techy Coronado Salazar, José Felipe de la Barra Barrera, Víctor Joe Manuel Enríquez Sumerinde, Francisco Manuel Fernández Reforme, Pedro David Franco Apaza, Juan Riquelme Guillermo Piscoya, Cecilia Milagros León Velásquez, Manuel Federico Loyola Florián, Francisco Celis Mendoza Ayma, Galileo Galilei Mendoza Calderón, Carlos Eduardo Merino Salazar, Juan Carlos Paredes Bardales, Roger Pari Taboada, Emperatriz Elizabeth Pérez Castillo, William Fernando Quiroz Salazar, Víctor Raúl Reyes Alvarado, Richard Rodríguez Alvan, Jorge Hernán Ruiz Arias, Ana Elizabeth Sales del Castillo, Alfredo Salinas Mendoza, Eduardo Sumire López, Julio Ernesto Tejada Aguirre, María Luz Vásquez Vargas, Tulio Eduardo Villacorta Calderón, Juan Rodolfo Segundo Zamora Barboza, Aldo Enrique Zapata López y Rene Santos Zelada Flores, de los diferentes distritos judiciales de nuestro querido territorio. Las discusiones fueron arduas y de ahí tenemos

destacados magistrados que siguen trabajando en el tema de ciber crimen desde cada punto de vista como veremos en el desarrollo del trabajo cotidiano.

En efecto, los señores magistrados arriba nombrados, durante muchos años dieron el fuste necesario en la capacitación hasta la total implementación del Código Procesal Penal en todo el Perú, agradecimiento eterno por su descollante entrega al trabajo académico pese a la carga procesal que inunda cada despacho.

Finalmente, en este extremo, se destaca que el Centro de Investigaciones Judiciales del Poder Judicial, en comunión de ideas con el Concejo de Europa, convocaron a magistrados interesados tanto del Poder Judicial como del Ministerio Publico a ser convocados en el nuevo grupo de "Formador de Formadores" en "**Ciber delincuencia y pruebas electrónicas para jueces y fiscales**" a nivel nacional, donde destacan profesionales de gran Valia, tanto del Ministerio Publico como del Poder Judicial, como Consuelo Cecilia Aquize Diaz de Montes de Oca, Roger Pari Taboada, William Fernando Quiroz Salazar, Pedro David Franco Apaza, Máximo Belisario Torres Cruz, Jaime Francisco Coaguila Valdivia, Jimmy Alan Manchego Enríquez, Galileo Galilei Mendoza Calderón, María Esther Felices Mendoza, Cesar Augusto Riveros Ramos, Walter Agustín Jiménez Basilio, dignos jueces de diferentes distritos judiciales, todos ellos honran al proceso de capacitación que en efecto resulta difícil en tiempos de carga procesal, nuestro agradecimiento a tan dilectos colegas que conjuntamente con el autor integra dichos equipos de Formador de Formadores, es por ello que el reconocimiento a los capacitadores que vienen formándonos y el resultado de ese esfuerzo es la publicación del presente trabajo, gracias maestros: Cristos Velazco San Martin, que ha tenido la bondad de emitir el prefacio en esta obra, Antonio Piña Alonso, destacado maestro y magistrado español, a nuestra mentora Catalina Stroe del Consejo de Europa y Glacy +.

Ofrecemos las disculpas del caso, por la licencia que nos ha permitido en la introducción hacer mención de tan dilectos personales de la juridicidad mundial, no sin antes, agradecer a todos quienes nos aportaron con ideas y logística entera, por ello mi reconocimiento eterno a la familia que abrazó el derecho con denuedo, desde don Bonifacio Meneses Romero el patriarca, los hombres y mujeres de derecho como Gloria Rosario, Roger Fernando, Estela Rosemary, Susam del Rosario, Fiorela Natalie, María Belen, Jeffer, Betty Victoria, todos en ese tándem como nuestro prologuista señaló, Meneses & Meneses.

Finalmente, el fin de la presente obra es brindar a los operadores del sistema penal, un estudio sobre el tratamiento de la cibercriminalidad, desde el punto de vista de la política criminal, criminología, ciberseguridad, derecho penal, derecho procesal penal y la asistencia penal internacional. Todo esto no seria posible

sino, por la decidida actuación y desarrollo de la difusión planteada en la Conferencia Internacional Iberoamericana sobre Protección de Datos Personales: **"Inteligencia Artificial y Privacidad: Un enfoque humano para la tecnología"** en mayo del 2024, organizado por la Universidad Católica de Cuenca - Ecuador, gracias señor rector por su apoyo, además a la Universidad Pontificia de Salamanca e Instituto Iberoamericano de Justicia.

Lima – Perú, verano del 2024

Los autores.