

THOMSON REUTERS
LA LEY



ESTE LIBRO INCLUYE UNA
VERSIÓN ELECTRÓNICA

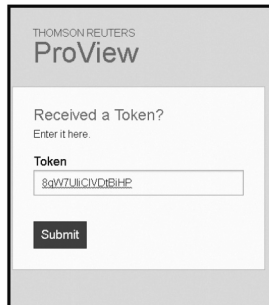
THOMSON REUTERS
ProView™

SI NO TIENE
UNA CUENTA
ONEPASS

- 1** - Ingresar a <https://onepass.thomsonreuters.com> y clicar en "Crear perfil **OnePass**".
- 2** - Registrar un e-mail personal para asociar la cuenta y, a continuación, completar los datos requeridos.
- 3** - Una vez creada la cuenta, cerrar sesión y dirigirse al mail personal para activar el número *token*.

SI YA CREÓ
SU CUENTA
ONEPASS

- 1** - Validar el número de token recibido por mail haciendo clic en el enlace enviado.



The screenshot shows a web interface for Thomson Reuters ProView. At the top, it says 'THOMSON REUTERS ProView'. Below that, a box contains the text 'Received a Token? Enter it here.' There is a text input field with the token '8aW7UjCIVdRiHP' entered. A 'Submit' button is located at the bottom of the input area.

- 2** - Luego, ingresar a la cuenta **OnePass** y confirmar el token haciendo clic en *submit*. Aparecerá la imagen de la tapa del libro adquirido.

- 3** - Acceder al material comprado a través de la Biblioteca Digital **ProView** con el usuario y la contraseña creados previamente en **OnePass**.

- 4** - La Biblioteca Digital **ProView** está disponible para varios soportes.



• **Navegador:** Acceder a través de www.proview.thomsonreuters.com



• **Tableta o IPAD:** Descargar la aplicación "Thomson Reuters ProView" desde iTunes Store o Play Store, según corresponda



• **Aplicación de escritorio para PC o MAC:** Descargar la aplicación en <https://proview.thomsonreuters.com>

Por consultas sobre el proceso de activación de la versión electrónica puede comunicarse al teléfono **0-810-222-5253**

CONOZCA Y APROVECHE TODAS LAS FUNCIONALIDADES DE UN **LIBRO ELECTRÓNICO EN PROVIEW**



SELECCIONE Y DESTAQUE TEXTOS

Haga anotaciones y escoja los colores para organizar sus notas y resaltados



USE EL TESAURO PARA ENCONTRAR INFORMACIÓN

Al comenzar a escribir un término, aparecerán las distintas coincidencias del índice del Tesauro relacionadas con el término buscado



HISTORIAL DE NAVEGACIÓN

Vuelva a las páginas por las que ya haya navegado



ORDENAR

Organice su biblioteca por: título (orden alfabético), tipo (libros y revistas), editorial, jurisdicción o área del Derecho, libros leídos recientemente o los títulos propios



CONFIGURACIÓN Y PREFERENCIAS

Escoja la apariencia de sus libros y revistas en ProView cambiando la fuente del texto, el tamaño de los caracteres, el espaciado entre líneas o la relación de colores



MARCADORES DE PÁGINA

Cree un marcador de página en el libro cliqueando en el ícono de *marcador de página* situado en el extremo superior derecho de la página



BÚSQUEDA EN LA BIBLIOTECA

Busque en todos sus libros y obtenga resultados acerca de los libros y revistas en donde los términos fueron encontrados y las veces que aparecen en cada obra



IMPORTACIÓN DE ANOTACIONES A UNA NUEVA EDICIÓN

Transfiera todas sus anotaciones y marcadores de manera automática



SUMARIO NAVEGABLE

Sumario con accesos directos al contenido

Nota: no todas las funcionalidades están disponibles en todos los libros.

TECNOLOGÍA INFORMÁTICA E INVESTIGACIÓN CRIMINAL

HERNÁN BLANCO

TECNOLOGÍA INFORMÁTICA E INVESTIGACIÓN CRIMINAL

USO DE HACKERS POR EL ESTADO - SPYWARE
LEGAL - NUEVAS TECNOLOGÍAS DE VIGILANCIA
- ACCESO REMOTO A DATOS INFORMÁTICOS
- BÚSQUEDAS TRANSFRONTERIZAS
- DESENCRIPTACIÓN COMPULSIVA -
ANONIMIZACIÓN Y AGENTE ENCUBIERTO
DIGITAL - BIG DATA Y SOFTWARE PREDICTIVO -
OBTENCIÓN, RESGUARDO Y ANÁLISIS FORENSE
DE LA EVIDENCIA DIGITAL - DEEP FAKES -
PRUEBA INFORMÁTICA APORTADA
POR HACKERS

THOMSON REUTERS

LA LEY

Blanco, Hernán
Tecnología informática e investigación criminal: uso de hackers por el estado - spyware legal-nuevas tecnologías de vigilancia - acceso remoto a datos informáticos - búsquedas transfronterizas - descriptación compulsiva - anonimización y agente encubierto digital - big data y software predictivo - obtención, resguardo y análisis forense de la evidencia digital - deep fakes - prueba informática aportada por hackers / Hernán Blanco.- 1a ed.- Ciudad Autónoma de Buenos Aires: La Ley, 2020.
896 p.; 24 x 18 cm.

ISBN 978-987-03-3966-3

1. Estrategias de la Investigación. 2. Procesos Penales.
3. Tecnología Informática. I. Título.
CDD 345.0504

© Hernán Blanco, 2020
© de esta edición, La Ley S.A.E. e I., 2020
Tucumán 1471 (C1050AAC) Buenos Aires
Queda hecho el depósito que previene la ley 11.723

Impreso en la Argentina

Todos los derechos reservados

Ninguna parte de esta obra puede ser reproducida o transmitida en cualquier forma o por cualquier medio electrónico o mecánico, incluyendo fotocopiado, grabación o cualquier otro sistema de archivo y recuperación de información, sin el previo permiso por escrito del Editor y el autor.

Printed in Argentina

All rights reserved

No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording or by any information storage or retrieval system, without permission in writing from the Publisher and the author.

Tirada ### ejemplares

ISBN 978-987-03-3966-3

SAP 42780330

Las opiniones personales vertidas en los capítulos de esta obra son privativas de quienes las emiten.

REFERENCIAS DEL AUTOR

Abogado. Secretario letrado en la Corte Suprema de Justicia de la Nación.

Se desempeñó como secretario de la sala IV de la Cámara Federal de Casación Penal, en la Unidad Fiscal de Investigación de Delitos Tributarios y Contrabando (UFITCO) y en la SEDRONAR. Autor de libros y múltiples artículos.

Expositor en universidades, foros y conferencias.

ÍNDICE

Prologo, por Marcos Salt	XIII
--------------------------------	------

CAPÍTULO 1

DE LA CONTRACULTURA AL ESTADO. EL CAMINO HACIA EL *HACKEO* GUBERNAMENTAL

1.1. El origen de los <i>hackers</i> . Aparición y persistencia de la “ética <i>hacker</i> ”...	1
1.2. El surgimiento del <i>hacker</i> “intruso”. Los <i>hackers</i> de “sombrero negro”, “sombrero blanco” y “sombrero gris”	8
1.3. El <i>hacktivismo</i> y las modernas agrupaciones de <i>hackers</i>	22
1.4. El surgimiento del <i>hackeo</i> estatal y paraestatal. “AAPs” y cibergue-rras. <i>Hackers</i> al servicio del Estado	37
1.5. El uso de <i>hackers</i> para colaborar con el Estado en la investigación de delitos	54

CAPÍTULO 2

GOING DARK. PROBLEMAS Y ALTERNATIVAS PARA EL MONITOREO DE COMUNICACIONES EN EL NUEVO AMBIENTE TECNOLÓGICO

2.1. Apogeo y ocaso del modelo actual de interceptación de comunica-ciones. El problema del <i>going dark</i> (“quedar a oscuras”).....	61
2.2. Principales amenazas tecnológicas a la continuidad del modelo actual de interceptación de comunicaciones	71
2.3. Propuesta de solución. <i>Hackeo</i> legal mediante el aprovechamiento de vulnerabilidades en los sistemas informáticos.....	88
2.4. Implementación técnica del <i>hackeo</i> legal. Problemas y soluciones..	102
2.5. Validez constitucional del <i>hackeo</i> legal. Aplicación analógica	118
2.6. Implementación legal del <i>hackeo</i> legal. Problemas procesales.....	143

CAPÍTULO 3

GOING BRIGHT. LAS VENTAJAS PARA LA INVESTIGACIÓN EN EL NUEVO ESCENARIO TECNOLÓGICO (I): VIGILANCIA ELECTRÓNICA DE LOS "RASTROS DIGITALES"

3.1. Situación real de las facultades estatales. <i>Going dark vs. going bright</i>	155
3.2. La recolección de "datos de envoltorio" como herramienta de investigación. La controversia en torno a la "doctrina de los terceros"....	164
3.3. El problema de la recolección o retención masiva de datos	186
3.4. Métodos de obtención directa de información sobre comunicaciones. Uso de "IMSI catchers"	201
3.5. Interceptación directa de tráfico de datos en internet	218
3.6. La recolección de "Información de Fuente Abierta" (<i>Open Source Intelligence</i> - OSINT).....	228

CAPÍTULO 4

GOING BRIGHT. LAS VENTAJAS PARA LA INVESTIGACIÓN EN EL NUEVO ESCENARIO TECNOLÓGICO (II). NUEVAS HERRAMIENTAS DE VIGILANCIA ESTATAL

4.1. La evolución tecnológica y su impacto en la aparición o evolución de los métodos de vigilancia estatales.....	249
4.2. Monitoreo de los movimientos de los ciudadanos mediante dispositivos GPS.....	255
4.3. Herramientas de vigilancia acústica. Micrófonos ocultos	262
4.4. Nuevas herramientas de video vigilancia. Sistemas de CCTV, cámaras termales, cámaras corporales y lectores de chapas patente.....	278
4.5. Vigilancia mediante aeronaves no tripuladas.....	309
4.6. La "Internet de las cosas" (IoT) como herramienta para la vigilancia estatal.....	330

CAPÍTULO 5

LA "COMPUTACIÓN EN NUBE" Y EL MOVIMIENTO TRANSFRONTERIZO DE EVIDENCIA INFORMÁTICA

5.1. El nuevo contexto tecnológico y su influencia en la obtención de evidencia almacenada en sistemas informáticos.....	343
--	-----

5.2. Crisis del principio de territorialidad frente al fenómeno de la pérdida de (conocimiento) de la locación de los datos informáticos	358
5.3. Métodos para la obtención de evidencia digital localizada en el extranjero: cooperación internacional.....	369
5.4. Métodos para la obtención de evidencia digital localizada en el extranjero (II): obtención directa mediante requerimientos a privados	378
5.5. Métodos para la obtención de evidencia digital localizada en el extranjero (III): obtención directa mediante acceso remoto a los datos.....	398
5.6. Necesidad de un replanteo del principio de territorialidad. Puntos de partida y problemática	424

CAPÍTULO 6

HERRAMIENTAS PARA CONTRARRESTAR EL ANONIMATO EN LA INTERNET

6.1. Herramientas que favorecen el anonimato en la internet.....	437
6.2. Actividad ilícita favorecida por el anonimato en la red. El recurso a las criptomonedas	451
6.3. Herramientas tecnológicas para contrarrestar el anonimato en la internet	462
6.4. Problemas procesales derivados del uso de las herramientas tecnológicas contra el anonimato en la red.....	482
6.5. El agente encubierto en el entorno digital.....	504

CAPÍTULO 7

LA GARANTÍA CONTRA LA AUTOINCRIMINACIÓN Y LA DESENCRIPTACIÓN COMPULSIVA DE DATOS

7.1. Encriptación de datos almacenados en equipos electrónicos y esteganografía.....	533
7.2. Opciones del Estado para acceder por sus propios medios a datos protegidos por encriptación o esteganografía	546
7.3. Elusión del problema de la encriptación mediante la cooperación (voluntaria u obligatoria) del sector privado. Las “criptoguerras”..	562
7.4. Desencriptación compulsiva por orden judicial (I). Marco jurisprudencial en orden al alcance de la garantía contra la autoincriminación en relación con la entrega de documentos.....	580

7.5. Descriptación compulsiva por orden judicial (II): aplicación de la garantía contra la autoincriminación en el nuevo contexto tecnológico	600
7.6. Descriptación compulsiva por orden judicial (III): la controversia en la doctrina estadounidense	611

CAPÍTULO 8

NUEVAS AMENAZAS A LA PRIVACIDAD. *BIG DATA* Y POLÍTICAS POLICIALES PREDICTIVAS

8.1. El derecho a la privacidad y la requisita (sin orden judicial) de <i>smartphones</i> en el marco de un arresto	625
8.2. La doctrina de <i>Plain View</i> en el análisis forense de evidencia digital ...	637
8.3. <i>Big data</i> e investigación penal. El problema de la explotación de perfiles creados en bases de datos privadas.....	665
8.4. El problema de la protección efectiva de los datos personales en el contexto del <i>big data</i> . Hábeas data y ley 25.326	691
8.5. Uso de <i>big data</i> para el desarrollo de políticas de policía predictiva. Algoritmos predictivos	702

CAPÍTULO 9

CUESTIONES RELATIVAS A LA RECOLECCIÓN, ANÁLISIS Y VALORACIÓN DE PRUEBA INFORMÁTICA

9.1. Recolección de evidencia digital y cadena de custodia. Protocolos de actuación para las fuerzas de seguridad	723
9.2. La cadena de custodia y su importancia con relación a la evidencia digital. Consecuencias de su ruptura	742
9.3. Utilidad y confiabilidad de la prueba digital en el proceso penal	755
9.4. La prueba pericial informática	767
9.5. Validez de la prueba de origen ilícito incorporada por terceros	791

ÍNDICE BIBLIOGRÁFICO

.....	819
-------	-----