

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

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
-------	-----