

HELIODORO FIERRO-MÉNDEZ

PRUEBA ILÍCITA

**Interceptación de comunicaciones y
registro de computadores**



EDICIONES DOCTRINA Y LEY LTDA
Bogotá D.C. - Colombia

TABLA DE CONTENIDO

	Pág.
<i>Reflexión</i>	1
TÍTULO PRIMERO	
LA INFORMACIÓN	
CAPÍTULO PRIMERO	
LA COMUNICACIÓN	
I. Elementos de la comunicación	8
A. El transmisor	8
B. El canal de transmisión o medio de comunicación	9
C. Receptor	9
II. Tipos de comunicación	10
A. Simplex	10
B. Duplex o semi-duplex	10
C. Full-duplex	10
III. Contaminación de la señal	10
A. Distorsión	11
B. Interferencia	11

C.	Ruido	11
D.	Fuentes	13
1.	De ruido	13
a.	Ruido térmico (<i>Thermal Noise</i>)	13
b.	Ruido de choque (<i>Shot Noise</i>)	13
c.	Ruido atmosférico (<i>Atmospheric Noise</i>)	13
2.	De interferencia	13
3.	Otros tipos de interferencia	14
a.	Interferencia de canales adyacentes	14
b.	Efecto de captura	14
IV. ⁹	Variaciones técnicas de la comunicación	15
A.	Modulación	15
1.	Necesidad de modular las señales	15
2.	Clases de modulación	16
B.	Demodulación	16
C.	Señales de transmisión y señales de datos	16

CAPÍTULO SEGUNDO

MEDIOS DE COMUNICACIÓN

I.	Clasificación de los medios de comunicación	19
A.	Medios confinados	20
1.	Alambre	20
2.	Cable coaxial	21
3.	Cable par trenzado	22
4.	Fibra óptica	25
5.	Guía de onda	26
B.	Medios no confinados o no físicos	29
1.	Radio frecuencia	30
2.	Microondas	31

33	3. Satélite	32
33	a. Satélites orbitales	35
37	b. Satélites geoestacionarios	36
37	c. Satélites Geo, Meo y Leo	37
37	1) Geo	37
37	2) Meo	37
38	3) Leo	38
38	d. Estaciones satelitales terrestres	38
39	4. Transmisiones láser de infrarrojo	39
40	5. Telefonía celular	40
42	a. FDMA (Acceso múltiple por división de frecuencias, <i>Frequency Division Multiple Access</i>)	42
42	b. TDMA (Acceso múltiple por división de tiempo, <i>Time Division Multiple Access</i>)	42
44	c. CDMA (Acceso múltiple por división de código, <i>Code Division Multiple Access</i>)	44
45	d. PCS	45
45	1) Primera generación (1G)	45
46	2) Segunda generación (2G)	46
47	3) Tercera generación 3G	47
48	C. Espectro electromagnético	48
49	II. Red conmutada	49
50	A. Componentes de una red de computadores	50
50	1. <i>Software</i> de aplicaciones	50
50	2. El <i>software</i> de red	50
50	3. El <i>hardware</i> de red	50
51	B. Tipos de conexiones de red	51
51	1. Conexiones físicas	51
51	2. Conexiones lógicas o virtuales	51
51	C. Tipos de redes	51
52	D. Nodos de conmutación	52

52	1. Circuitos físicos	53
52	2. Circuitos virtuales	53
53	E. Parámetros que definen una red	54
53	1. Topología	54
53	2. Tipos de redes inalámbricas	56
53	3. Tipos de redes basadas en la distancia de cobertura	60
53	a. LAN	60
53	b. CAN	62
53	c. MAN	63
53	d. WAN	63
53	e. WLAN y WPAN	63
53	4. Métodos de acceso al medio (LAN)	64
53	5. Testigo de control (<i>token passing</i>)	64
53	6. Direccionamiento IP (<i>IP Addressing</i>)	65
53	7. Clases de direcciones IP	66
53	a. Dirección IP clase A	66
53	b. Dirección IP clase B	66
53	c. Dirección IP clase C	67
53	8. Dirección IP móvil	67
53	9. Máscaras de subred (<i>subnet mask</i>)	71
53	F. Redes de conmutación de circuitos	71
53	1. Establecimiento del circuito	72
53	2. Transferencia de datos	72
53	3. Cierre del circuito	72
53	III. Modos de transmisión de datos en medios informáticos	72
53	A. Paralelo	72
53	B. Serie	73
53	1. Transmisión asincrónica	73
53	2. Transmisión sincrónica	74
53	IV. Banda base	74

A.	Clasificación de la banda base	74
1.	Unipolares	74
2.	Polares	75
3.	Bipolares	75
B.	Transmisión en banda base	75

CAPÍTULO TERCERO

LA WEB COMO SISTEMA DE INFORMACIÓN

I.	Objetivo final de los servicios <i>web</i>	77
II.	Sistema de gestión de contenidos	80

TÍTULO SEGUNDO

LA BÚSQUEDA DE DATOS

CAPÍTULO PRIMERO

LA MINERÍA DE LA INFORMACIÓN

I.	Los datos	84
A.	Selección y recopilación de datos	84
B.	Tratamiento previo de los datos	85
C.	Transformación de los datos	85
D.	Análisis de las inferencias sobre los datos	85
E.	Tipos de minería de textos <i>web</i> (<i>web mining</i>)	86
1.	Ficheros <i>logs</i>	86
2.	Minería de estructura	87
3.	Minería de uso	87
II.	Descubrimiento de información en bases de datos	88

CAPÍTULO SEGUNDO

RECUPERACIÓN DE INFORMACIÓN

I.	Componentes esenciales de búsqueda	94
A.	Documentos estructurados	94
B.	Bases de datos donde estén almacenados los documentos	94
	1. Según la variabilidad de los datos almacenados	95
	a. Bases de datos estáticas	95
	b. Bases de datos dinámicas	96
	2. Según el contenido	96
	a. Bases de datos bibliográficas	96
	b. Bases de datos de texto	96
	c. Banco de imágenes, audio, video, multimedia, etc.	96
	3. Base de datos relacional	96
II.	Herramientas de búsqueda	97
A.	Buscadores generales	97
B.	Directorios	98
	1. El usuario no sabe mucho sobre el tema en concreto	98
	2. Directorio y motores especializados	98
C.	Metabuscadore	98
D.	Buscadores selectivos	99
E.	Programa para búsqueda	99
F.	Agentes inteligentes	99
G.	Metadatos	99
III.	Lenguajes de indización y control terminológico	100
A.	Índices	100
B.	Palabras clave (<i>keywords</i>)	100
C.	Meta <i>keywords</i>	101
D.	Tesauros	101
IV.	1. Componentes	101

2.	Relaciones	101
IV.	Lenguajes de interrogación y ecuaciones de búsqueda	102
V.	Navegación versus recuperación de información	102
VI.	Técnicas de recuperación de información	103
A.	Sistemas de recuperación de lógica difusa	103
B.	Técnicas de ponderación de términos	104
C.	Técnica de <i>clustering</i>	104
D.	Técnicas de retroalimentación por relevancia	104
E.	Técnicas de <i>stemming</i>	105
F.	Técnicas lingüísticas	105
CAPÍTULO TERCERO		
LA MICROFONÍA ENCUBIERTA		
I.	Verdades y mentiras en materia de interceptaciones	108
II.	Interceptación de celulares	110
A.	Monitoreo de audio ambiental	111
B.	Monitoreo de envío y recepción de SMS	111
C.	Escucha de comunicación celular	112
D.	Alerta de llamadas entrantes y salientes vía SMS	112
E.	Localización geográfica por medio de red celular	112
F.	Notificación de apagado y encendido	113
G.	Control de comandos vía SMS - Lista de comandos vía SMS:	113
III.	Aparatos o servicios que pueden transmitir conversaciones	114
CAPÍTULO CUARTO		
EMBATES, DEBILIDADES Y PROTECCIÓN INFORMÁTICA		
I.	Clases de asaltos informáticos	117
A.	Ataques de intromisión	117

101	B. Ataque de espionaje en línea	117
501	C. Ataque de interceptación	118
501	D. Ataque de modificación	118
II.4	II. <i>Phishing</i>	119
III.	III. <i>Software</i> espía	119
IV.	IV. <i>Spammers</i>	120
V.1	V. Los <i>password</i> o contraseñas	120
VI.	VI. Ingeniería social	121
VII.	VII. Almacenaje indebido	121
VIII.	VIII. Ataques por fuerza bruta	121
IX.	IX. Monitorización del teclado	122
X.	X. Monitorización de la red y ataques por medio de accesos grabados	122
XI.	XI. Accesos no autorizados	122
XII.	XII. Mecanismos de confidencialidad	123
101	A. Encriptación	123
111	B. Encubrimiento del tamaño (<i>data padding</i>)	123
111	C. Encubrimiento del tráfico (<i>traffic padding</i>)	123
XIII.	XIII. Integridad	123
112	A. <i>Testwords</i>	124
112	B. Sellos o firmas	124
113	C. Encriptación	124
113	D. Integridad de la secuencia	125
XIV.	XIV. No-repudiación	125
114	A. No repudiación del origen	125
114	B. No repudiación de la recepción	125
114	C. Fases del proceso de no repudiación	126
117	1. Solicitud de servicio	126
117	2. Generación de evidencia	126
117	3. Transferencia/Almacenamiento de la evidencia	126

4.	Verificación de la evidencia	127
5.	Resolución de disputas	127
XV.	<i>Firewalls</i>	127
1.	<i>Firewall</i> de filtro de paquetes	128
2.	<i>Gateways</i> de aplicación	129
3.	<i>Firewall</i> de confianza (<i>trusted gateway</i>)	130
4.	<i>Firewalls</i> internos	130
XVI.	Sistemas criptográficos	131
A.	Tipo de operaciones para transformar el texto plano en texto cifrado	131
1.	Técnicas de sustitución	132
2.	Técnicas de transposición	132
B.	Número de claves utilizado	133
C.	Forma de procesar el texto plano	133
1.	Cifrador de bloque	133
2.	Cifrador de corriente de datos (<i>stream</i>)	133
D.	Métodos de encriptación	133
1.	Encriptación simétrica	133
2.	Encriptación asimétrica	134

TÍTULO TERCERO

INTIMIDAD Y EXPECTATIVA RAZONABLE

CAPÍTULO PRIMERO

DERECHO A LA INTIMIDAD

I.	Núcleo esencial del derecho a la intimidad	141
II.	Grados de intimidad	144
A.	Intimidad personal	145
B.	Intimidad familiar	145

C. Intimidad social 146

D. Intimidad gremial 146

III. Formas de vulnerar el derecho a la intimidad 147

IV. Principios que sustentan la protección del derecho a la intimidad 148

A. Principio de libertad 149

B. Principio de finalidad 149

C. Principio de necesidad 150

D. Principio de veracidad 150

E. Principio de integridad 150

V. Interés general, interés social y derechos individuales 152

CAPÍTULO SEGUNDO

LA EXPECTATIVA RAZONABLE DE INTIMIDAD

I. Conductas públicas 169

II. Personas de vida pública 170

III. Expectativa de intimidad de quien está de visita en una morada 171

CAPÍTULO TERCERO

STANDING

Generalidades 173

DERECHO A LA INTIMIDAD

A. Intimidad personal 176

B. Intimidad familiar 176

C. Intimidad profesional 176

D. Intimidad sexual 176

E. Intimidad de la información 176

F. Intimidad de la imagen 176

G. Intimidad de la voz 176

H. Intimidad de la identidad 176

I. Intimidad de la libertad 176

J. Intimidad de la dignidad 176

K. Intimidad de la vida 176

L. Intimidad de la muerte 176

TÍTULO CUARTO

PROBLEMAS LEGALES DE LA INTERCEPTACIÓN DE COMUNICACIONES

CAPÍTULO PRIMERO

INTERCEPTACIÓN DE COMUNICACIONES EN LA LEY PROCESAL PENAL

I.	Derecho a la intimidad y derecho a la información	179
II.	La inviolabilidad de las comunicaciones privadas y la libertad personal	180
III.	Las intervenciones mediante registros	183
A.	La búsqueda selectiva de información en bases de datos no es una especie del registro	183
B.	Tipología de información que se maneja a través de las bases de datos	184
C.	El recaudo de información debe acatar los preceptos constitucionales	185
IV.	Búsqueda de información confidencial en bases de datos	188
A.	Las medidas que afectan derechos fundamentales requieren autorización previa	189
B.	La búsqueda selectiva en bases de datos y su ubicación en el <i>habeas data</i>	192
V.	La correspondencia y las comunicaciones privadas	194
VI.	La información de teléfono celular y la SIM CARD	197

CAPÍTULO SEGUNDO

INCAUTACIÓN, REGISTRO DE COMPUTADORES Y CADENA DE CUSTODIA EN LA LEY PENAL

I.	Normas sobre cadena de custodia	204
----	---------------------------------------	-----

A.	Código de Procedimiento Penal	204
B.	Lo establecido por la Fiscalía General de la Nación	204
1.	Manejo del lugar de los hechos	206
2.	Fijación del lugar de los hechos	207
3.	Recolección, embalaje y rotulado de los elementos materia de prueba o evidencias	207
4.	Envío de elementos y evidencias al almacén transitorio	209
5.	La documentación del sistema de cadena de custodia se regula en los siguientes términos	212
6.	Algunas formas de recolección, embalajes y recomendaciones prácticas para el manejo de elementos materia de prueba o evidencias físicas	214
C.	Antecedentes jurisprudenciales	220
D.	La regla de exclusión y la prueba ilícita según la Corte Constitucional	226
II.	El derecho a la intimidad y la intervención sin control judicial de los discos duros	226
CAPÍTULO TERCERO		
VIGILANCIA Y CONTROL DEL ESPECTRO ELECTROMAGNÉTICO		
I.	Naturaleza y alcances de la vigilancia y el control del espectro electromagnético	233
II.	Labores de inteligencia que corresponden a la Policía Nacional	242
III.	Límites a las labores de monitoreo del espectro electromagnético y al ejercicio de las labores de inteligencia	249
IV.	El monitoreo pasivo	258

INCALCULACIÓN, REGISTRO DE
COMPUTADORES Y CADENA DE
CUSTODIA EN LA LEY PENAL