

ÍNDICE GENERAL

Pág.

INTRODUCCIÓN

1. Marco teórico de referencia. Relaciones existentes entre Informática y Derecho	1
2. Informática jurídica.....	7
2.1. Antecedentes de la Informática jurídica	8
2.2. Definiciones y clasificaciones de la Informática jurídica	11
2.3. Clasificación	12
2.4. Informática jurídica documental	12
2.4.1. La aplicación técnico-jurídica	12
2.4.1.1. Indexación.....	13
2.4.1.2. Texto completo.....	13
2.4.1.3. <i>Abstract</i>	13
2.5. Informática jurídica de gestión.....	14
2.5.1. Clasificación	14
2.5.1.1. Informática jurídica registral	14
2.5.1.2. Informática jurídica operacional.....	15
2.6. Informática jurídica decisional.....	17
3. Derecho informático	19
3.1. Contenido.....	20
3.2. Concepto	37

CAPÍTULO I

INTERNET Y NOMBRES DE DOMINIO

1. Introducción	43
1.1. Internet. Aspectos técnicos	43
1.1.1. Red y redes.....	43
1.1.1.1. Red de área local (LAN)	43
1.1.1.2. Red de área abierta (WAN)	43
1.1.1.3. Red de redes (<i>Internetworks</i>)	44
1.1.1.4. Internet.....	44

	Pág.
1.1.1.5. <i>World Wide Web</i>	45
1.1.1.6. Historia de Internet	49
1.1.1.7. Estándares de la Web.....	54
1.1.2. Cómo se transmiten los datos en Internet	55
1.1.2.1. Protocolos de Internet.....	55
1.1.2.2. Dirección IP (<i>IP address</i>).....	56
1.1.2.3. Localizador Uniforme de Recursos (URL).....	58
1.1.2.4. Dirección IP. Versiones.....	59
1.1.2.5. Protocolo de Internet versión 6 (IPv6)	59
1.1.3. Conversión de números a palabras	61
1.1.3.1. Nombre de Dominio de Internet.....	62
1.1.3.2. Sistema de Nombres de Dominio.....	63
2. Asignación de números y nombres de dominio de Internet	64
2.1. Historia de la administración de los nombres de dominio	64
2.2. Clases de nombres de dominio	72
2.2.1. Nombres de Dominio de Nivel Superior (TLD).....	73
2.2.2. Nombres de dominio genéricos.....	75
2.2.3. Dominios de segundo nivel	78
2.2.4. Organismos vinculados al registro de Nombres de Dominio de Internet.....	79
2.2.4.1. IANA	79
2.2.4.2. LatinoamerICANN	79
2.2.4.3. LACLTD	79
2.2.4.4. InterNIC.....	79
2.2.5. Dominio de Europa	80
2.2.6. Nombres de dominio internacionalizados (IDNA).....	80
2.2.7. Nuevos dominios genéricos de alto nivel (gTLD)	83
2.3. Registro de nombres de dominio en Argentina.....	88
3. Nombres de Dominio de Internet.....	96
3.1. Naturaleza jurídica de los nombres de dominio	96
3.1.1. La función de los signos distintivos	100
3.1.2. Posiciones sobre la naturaleza jurídica de los nombres de dominio	103
3.1.3. Derecho al uso o goce del nombre de dominio.....	111
3.1.4. Embargabilidad (o no) de los nombres de dominio	113
3.1.4.1. El caso "Umbro"	113
3.1.4.2. Caso "Gimbutas"	115
4. Conflictos que suscitan los nombres de dominio.....	115
4.1. Caracterización de conductas típicas en el registro abusivo.....	117
4.1.1. Ciberocupación (" <i>cybersquatting</i> ").....	117
4.1.1.1. Definiciones de la OMPI	117
4.1.1.2. Conflictos con otros signos distintivos.....	120

	Pág.
4.1.2. Parasitismo (" <i>parasiting</i> ").....	120
4.1.3. El Segundo informe de la OMPI sobre Nombres de Dominio	121
4.1.4. La legislación norteamericana.....	125
4.2. El sistema de resolución de conflictos ICANN-OMPI (UDRP)	127
4.2.1. El Reglamento	129
4.2.2. Proveedores de servicios de solución de controversias.....	129
4.2.3. El procedimiento según la UDRP	132
4.2.4. Políticas adicionales	135
4.2.4.1. Política de Resolución de Disputas sobre Elegibilidad de Estatutos (CEDRP).....	135
4.2.4.2. Política de Reconsideración de Elegibilidad (ERP)	135
4.2.4.3. Política de Resolución de Disputas sobre Requisitos de Elegibilidad (ERDRP).....	136
4.2.4.4. La Política de Requisitos de Elegibilidad del Estatuto .ASIA (.ASIA CERP)	136
4.2.4.5. Política de Resolución de Disputas sobre Requisitos de Elegibilidad de .cat	137
4.2.4.6. La Política de Impugnación de Registros Defensivos de Propiedad Intelectual (IPDRCP)	137
4.2.4.7. Política de Impugnación de Requisitos (QCP).....	137
4.2.4.8. Política de Resolución de Disputas por Restricciones (RDRP)	138
4.2.4.9. Política de Oposición de los Titulares de Marcas en el Período Inicial de Solicitud de Registro de un Nombre de Dominio (STOP).....	138
4.2.4.10. Política de Impugnación Sunrise (o período de arranque)	139
4.2.4.11. Política de Resolución de Disputas por Transferencias (TDRP)	139
4.2.5. Reglas de solución de Disputas en otros países	139
4.3. Conflictos entre marcas y nombres de dominio de segundo nivel	147
4.3.1. Algunos casos resueltos por la OMPI.....	149
4.3.2. Conflictos suscitados entre partes domiciliadas en un mismo país. Principios aplicables	149
4.3.3. Prioridad de la marca "renombrada"	155
4.3.4. Conflictos entre dos nombres de dominio	157
4.3.5. Buena o mala fe	158
4.3.6. Conflicto entre signos distintivos notorios preexistentes y nombres de dominio. Nombre de dominio en uso. Mala fe	158
4.3.7. Conflicto entre signos distintivos notorios preexistentes y nombres de dominio - Mala fe	158
4.3.8. Conflicto entre nombres de dominio y nombres de personas famosas.....	159
4.3.9. Nombre de dominio que no está en uso. Mala fe	166

	Pág.
4.3.10. Otros casos de mala fe	167
4.3.11. Conflicto entre marcas y designaciones comerciales no notorias	167
4.4.12. Conflicto entre un nombre de dominio preexistente y marcas o designaciones posteriores	167
4.4. Prácticas óptimas sobre prevención y solución de controversias en materia de propiedad intelectual relacionadas con los ccTLD	168
4.4.1. Acuerdo de registro de nombres de dominio	169
4.4.2. Recopilación y disponibilidad de las informaciones que permitan establecer contacto con el titular del registro.....	170
4.4.3. Las consecuencias derivadas de proporcionar datos de contacto inexactos o no fiables.....	172
4.4.4. La repercusión de la protección del derecho de intimidad..	172
5. Breve análisis de la normativa argentina.....	173
5.1. Procedimiento de resolución administrativa de disputas.....	174
6. Jurisprudencia nacional.....	178
6.1. Primeros fallos judiciales argentinos	179
6.1.1. Caso "Freddo"	180
6.1.2. Caso "Pugliese"	182
6.1.3. Caso "Camuzzi"	184
6.1.4. Caso "Xenical"	184
6.1.5. El principio de prioridad puede ceder ante la marca	185
6.1.6. Revocación registro nombre de dominio por similitud con la marca	186
6.1.7. Es necesario acreditar un obrar de mala fe para la modificación o cancelación de la registración del nombre de dominio	187
6.1.8. Interés legítimo como factor de exclusión de la mala fe.....	187
6.1.9. Uso indebido de marca en una dirección de correo electrónico	190
6.1.10. Efectos de la registración en Nic-Argentina para el titular de una marca	190
6.1.11. Juez competente.....	193
6.1.12. Medidas cautelares	194
6.1.13. Posibilidad de generar confusión en la marca por el Nombre de dominio	195
6.1.14. No activación del nombre de dominio registrado.....	196
6.1.15. Valor de la "marca de hecho"	197
6.1.16. Buena fe en el registro de nombres de dominio	198
6.1.17. Aplicación de las Reglas de la Política Uniforme (UDRP) ...	198
6.1.19. Es necesario acreditar un obrar de mala fe para la modificación o cancelación de la registración del nombre de dominio	199
7. Casos resueltos por la OMPI.....	200

	Pág.
7.1. Marca no registrada y falta de prueba sobre uso notorio	200
7.2. Límites territoriales de la marca y nombres de dominio.....	202
7.3. No acreditación de la ausencia de interés legítimo	207
7.4. La oferta de los nombres de dominio al titular de una marca es demostrativo de la mala fe en el registro	207
8. Conclusiones	208
Bibliografía.....	209

CAPÍTULO II PROPIEDAD INTELECTUAL, PROGRAMAS DE COMPUTACIÓN Y BASES DE DATOS

1. Introducción	218
1.1. Propiedad Industrial.....	221
1.1.1. Patentes.....	222
1.1.2. Modelos de utilidad	230
1.1.3. Diseño industrial.....	232
1.1.4. La propiedad intelectual y los circuitos integrados	233
1.1.5. Marcas.....	235
1.1.6. Nombres comerciales	240
1.1.7. Indicaciones geográficas	243
1.1.8. Protección contra competencia desleal	244
1.1.9. La Organización Mundial de la Propiedad Intelectual	248
1.2. Derecho de autor	251
1.2.1. Antecedentes.....	252
1.2.2. Alcances del derecho de autor	261
1.3. Derechos conexos.....	262
1.4. Sociedades de gestión colectiva	264
2. <i>Software</i> o programa de computación.....	270
2.1. Breve historia del <i>software</i>	272
2.2. Código fuente.....	273
2.3. Algoritmo.....	274
2.4. Lenguaje de programación	276
2.5. Clasificación del <i>software</i>	280
2.5.1. <i>Software</i> de sistema	280
2.5.2. <i>Software</i> de programación	280
2.5.3. <i>Software</i> de aplicación.....	281
2.5.4. Proceso de creación del <i>software</i>	282
2.6. Protección legal de los programas de computación	284
2.6.1. Acuerdo ADPIC/TRIPs	287
2.6.2. Tratado de la OMPI.....	292

	Pág.
2.6.3. Conflictos sobre la extensión de la protección de derecho de autor al <i>software</i>	293
2.6.4. Protección del <i>software</i> . Ideas y expresión	301
2.6.5. Derecho comparado	306
2.6.5.1. Costa Rica	306
2.6.5.2. El Salvador.....	307
2.6.5.3. Guatemala.....	307
2.6.5.4. Honduras.....	308
2.6.5.5. Nicaragua	309
2.6.5.6. Panamá.....	310
2.6.5.7. República Dominicana	310
2.6.5.8. Uruguay	310
2.6.5.9. Brasil.....	311
2.6.5.10. Bolivia.....	313
2.6.5.11. Chile.....	315
2.6.5.12. Perú.....	316
2.6.5.13. Colombia	316
2.6.5.14. Ecuador	317
2.6.5.15. Venezuela	318
2.6.5.16. Paraguay	320
2.6.5.17. México	321
2.6.5.18. Comunidad Andina.....	324
2.6.5.19. Europa	326
2.6.5.20. Unión Europea.....	326
2.6.5.21. España	330
2.6.6. Situación en la República Argentina	336
2.6.6.1. Decreto 165/94.....	339
2.6.6.2. Ley 24.425.....	340
2.6.6.3. Antecedentes de la modificación de la ley 11.723... ..	343
2.6.6.4. Ley 25.036.....	345
2.6.6.5. Licencia de software.....	348
2.7. Tipos de plagio	355
2.7.1. "Piratería"	355
2.7.2. Plagio.....	364
2.7.3. Emulación de "look and feel"	366
3. Bases de datos	368
3.1. Protección jurídica de las bases de datos	369
3.1.1. El requisito de la originalidad	371
3.1.2. Las obras colectivas y el derecho de autor.....	377
3.1.3. Compilaciones, colecciones y bancos de datos.....	381
3.1.4. Selección o disposición como criterio de creatividad	384
3.1.5. El banco de datos como obra terminada	386

	Pág.
3.1.6. Originalidad en los bancos de datos	386
3.1.7. Fundamentos de las tesis doctrinarias.....	387
3.1.8. Crítica a la tesis que considera a los bancos de datos como obras protegibles	389
3.1.9. Las antologías y los bancos de datos	390
3.1.10. El caso Le Monde vs. Microfor	392
3.1.11. Originalidad en las antologías y en los bancos de datos.....	393
3.1.12. Legislación de Estados Unidos	393
3.2. La protección de los datos que integran un banco de datos	395
3.3. Bancos de datos que compran datos en bruto	400
3.4. Los derechos sobre los documentos de uso	402
3.4.1. Tesoros	403
3.4.2. El caso de la indexación o indización.....	406
3.4.3. El caso de los <i>abstracts</i>	406
3.4.4. El caso de los resúmenes	408
3.5. El caso de los corpus abiertos al gran público.....	409
3.6. El tratamiento de datos como objeto de derecho	410
3.7. El alcance de los derechos sobre el tratamiento de datos	412
3.8. Derechos sobre el banco y piratería	414
3.8.1. La jurisprudencia norteamericana sobre protección de las bases de datos	415
3.8.2. Jurisprudencia española	428
3.8.3. Tribunal de Justicia de la Comunidad Andina.....	429
3.8.4. Jurisprudencia nacional.....	437
3.9. Derechos conferidos al autor de la base de datos	440
3.10. Derechos sobre el banco y derechos de los clientes	442
3.10.1. El caso particular de los corredores de valores	444
4. El <i>software</i> libre.....	446
4.1. Los orígenes	446
4.2. El caso "Microsoft"	448
4.3. GNU y Linux	451
4.4. Código abierto (<i>Open Source</i>).....	456
4.5. <i>Software</i> libre.....	458
4.6. El Copyleft	460
4.7. Licencias F/OSS	461
4.7.1. La <i>Free Software Definition</i> (FSD).....	461
4.7.2. La <i>Open Source Definition</i> (OSD)	462
4.7.3. Similitudes y diferencias en las definiciones	463
4.7.4. Diversos tipos de licencias de <i>software</i> libre.....	464
4.7.4.1. La Licencia Pública General de GNU (GPL).....	465
4.7.4.2. GNU LGPL (Lesser General Public Licence).....	470
4.7.4.3. Licencia tipo BSD	471

	Pág.
4.8. Panorama actual.....	471
5. Internet y los derechos de propiedad intelectual.....	473
5.1. El impacto de las nuevas tecnologías en el derecho de autor.....	473
5.2. Técnicas utilizadas en Internet.....	479
5.3. Responsabilidad de los ISP o intermediarios.....	482
5.3.1. Posiciones enfrentadas.....	482
5.3.2. Regulaciones en el derecho comparado.....	484
5.4. Casos jurisprudenciales.....	490
5.4.1. El caso "Napster".....	492
5.4.2. El caso "Grokster" (Estados Unidos).....	493
5.4.3. El caso "KaZaA" (Australia).....	498
5.4.4. El caso "The Pirate Bay" (Suecia).....	499
5.4.5. El caso "Viacom vs. You Tube" (Estados Unidos).....	499
5.4.6. El caso "Infektor" (España).....	500
5.4.7. El caso "Baidu" (China).....	501
5.4.8. El caso "Italia Online" (Italia).....	501
5.4.9. Los casos "newzbin" (Gran Bretaña).....	501
5.4.10. Atipicidad del intercambio de archivos en Italia.....	502
5.4.11. El caso "Vélez" (Colombia).....	503
5.5. Jurisprudencia nacional.....	504
5.5.1. El caso "Taringa".....	504
5.5.2. El caso Cuevana.....	506
5.6. A manera de conclusión.....	507
Bibliografía.....	509

CAPÍTULO III

DOCUMENTO ELECTRÓNICO Y FIRMA DIGITAL

1. Concepto y objeto.....	519
1.1. El impacto tecnológico.....	519
1.2. Antecedentes. Estado actual de la cuestión.....	521
2. La forma y la prueba de los actos jurídicos.....	522
2.1. Forma.....	523
2.2. Prueba.....	525
3. Documento.....	526
3.1. Soporte documental.....	526
3.2. Modos de registración documental.....	527
3.3. Requisitos de un documento.....	528
3.3.1. Inalterabilidad.....	528
3.3.2. Autenticidad.....	528
3.3.3. Durabilidad.....	528
3.4. Aceptación jurídica del documento.....	529

	Pág.
3.5. La regulación del Código Civil respecto de los instrumentos públicos y privados.....	530
3.6. Firma.....	531
3.6.1. La firma ológrafa.....	531
3.7. Modernas técnicas de seguridad.....	532
3.7.1. Sistemas de criptografía.....	533
3.7.1.1. Sistemas de criptografía simétrica.....	537
3.7.1.2. Sistemas de criptografía asimétrica.....	537
3.7.2. Biometría.....	538
3.7.2.1. La autenticación biométrica.....	539
3.7.2.2. Tipos de Biometría.....	539
3.7.2.2.1. Biometría Estática.....	540
3.7.2.2.2. Biometría Dinámica.....	540
3.7.2.3. Criterios para utilizar la biometría como método de autenticación.....	540
3.7.2.4. Propiedades de los datos biométricos.....	540
3.7.2.5. Elementos de un sistema biométrico.....	541
3.7.2.6. Fases del procedimiento biométrico.....	541
3.7.2.7. Las huellas digitales.....	542
3.7.2.8. Geografía de la mano.....	542
3.7.2.9. Retina del ojo.....	543
3.7.2.10. El iris del ojo.....	543
3.7.2.11. La cara.....	543
3.7.2.12. La voz.....	544
3.7.2.13. Balance.....	544
4. El documento electrónico (o digital).....	545
4.1. Introducción.....	545
4.2. Documento digital en sentido estricto y en sentido amplio.....	546
4.3. Algunas precisiones técnicas.....	547
4.3.1. Electrónico y digital.....	548
4.3.2. Digitalización.....	548
4.4. El documento electrónico como instrumento privado.....	550
4.5. Valor probatorio del documento electrónico como instrumento privado.....	551
4.6. El documento electrónico como instrumento público.....	553
4.7. Autenticidad, inalterabilidad y seguridad del documento electrónico.....	554
5. Criterios de apreciación de la prueba.....	556
5.1. Convenciones sobre la carga de la prueba.....	557
5.2. Informática y medios de prueba.....	559
6. Firma digital o electrónica avanzada.....	564
6.1. Distintas acepciones.....	564

	Pág.
6.2. Infraestructura de Clave Pública (PKI)	565
7. Antecedentes nacionales	566
7.1. Anteproyecto de 1987	566
7.2. Artículo 30 de la ley 24.624 y Disposición Administrativa 43/96 ...	567
7.3. Decisión Administrativa JGM 43/96.....	572
7.3.1. Ámbito de Aplicación	572
7.3.2. Requisitos en general.....	575
7.3.3. Requisitos en cuanto a los documentos.....	575
7.3.4. Requisitos en cuanto al soporte.....	576
7.3.5. Procedimiento respaldatorio	577
7.3.6. Procedimiento de verificación.....	579
7.3.7. Registro	580
7.3.8. De la anulación	580
7.3.9. Documentos de terceros	581
7.3.10. Destrucción	582
7.3.11. Conservación y seguridad	582
7.3.12. Copias de la documentación digitalizada.....	583
8. Ley sobre Documento Electrónico y Firma Digital 25.506.....	583
8.1. Firma electrónica	586
8.2. Documento digital	588
8.3. Firma digital	589
8.3.1. Requisitos de validez	591
8.3.2. Remitente	592
8.4. Extensión del concepto de firma	593
8.5. Certificados digitales	594
8.6. Presunción de autoría	598
8.7. Presunción de integridad.....	599
8.8. Eficacia probatoria. Garantía de no repudio	600
8.9. Originales	600
8.10. Conservación de documentos	601
8.11. Exclusiones.....	601
8.11.1. Acto jurídico familiar	602
8.11.2. Algunas consideraciones sobre la exclusión de los actos jurídicos familiares.....	602
8.12. Conservación de documentos.....	606
8.13. Original	607
8.14. Certificador licenciado.....	608
8.15. Titulares de certificados digitales	615
8.16. Infraestructura de firma digital.....	616
8.17. Autoridad de Aplicación	618
8.18. Sistema de Auditoría	620
8.19. Comisión Asesora	621

	Pág.
8.20. Responsabilidad	622
8.21. Sanciones	625
8.22. Utilización por el Estado Nacional.	626
8.23. Código Penal	628
8.24. Glosario	628
9. Decreto 2628/2002	629
9.1. Diversos sistemas de firmas electrónica y digitales	631
9.2. Certificados emitidos por certificadores no licenciados	632
9.3. Generación, comunicación y archivo de documentos digitales....	633
9.4. Establecimiento de estándares tecnológicos.....	633
9.5. Comisión Asesora para la Infraestructura de Firma Digital	635
9.5.1. Consulta pública	635
9.6. Ente Administrador de Firma Digital	636
9.7. Oficina Nacional de Tecnologías de la Información (ONTI).....	637
9.7.1. Responsabilidad primaria.....	637
9.7.2. Acciones.....	638
9.7.3. Auditorías	642
9.7.4. Revocación de certificados.....	643
9.7.5. Obtención de la licencia.....	644
9.7.6. Plan de Cese de actividades y el Plan de Contingencia.	648
9.7.7. Autoridades de registro	650
9.8. Administración Pública Nacional.....	651
9.9. Glosario	653
10.1. Descripción general de la norma	655
10.2. Infraestructura de Firma Digital de la República Argentina (IFDRA - hoy IFDN)	659
10.3. Estándares tecnológicos.....	662
10.4. Certificadores licenciados.....	662
10.5. Registro de certificadores licenciados.....	664
10.6. Certificados de personas jurídicas	665
10.7. Auditorías	665
10.8. Aranceles y garantías.....	666
10.9. Seguros	666
10.10. Normas de procedimiento	667
10.11. Renovación.....	668
10.12. Cese de actividades.....	668
10.13. Defensa del usuario	669
10.14. Sanciones.....	670
10.15. Licenciamiento de certificadores	671
10.15.1. Deber de información	673
10.15.2. Contratos con los usuarios.....	674
10.15.3. Política de privacidad	674

	Pág.
10.15.4. Políticas de certificación y Manual de Procedimiento.....	674
10.15.5. Plan de seguridad.....	675
10.15.6. Comunicación con las autoridades de registro	675
10.15.7. Registro de eventos	675
10.15.8. Plan de cese de actividades.....	676
10.15.9. Plan de contingencias.....	676
10.15.10. Plataforma tecnológica y estándares determinados para los dispositivos.....	677
10.15.11. Políticas de certificación.....	677
10.15.12. Identificación y autenticación.....	684
10.15.13. Ciclo de vida del certificado	686
10.15.14. Controles de seguridad.....	688
10.15.15. Perfiles de certificados.....	689
10.15.16. Perfil mínimo de certificados y listas de certificados revocados.....	689
10.15.17. Resumen política de certificación y manual de procedimiento.....	691
10.15.18. Contenidos mínimos de acuerdos con suscriptores	693
10.15.19. Términos y condiciones con terceros usuarios.....	693
10.15.20. Contenidos mínimos de la política de privacidad.....	694
11. La situación en el Derecho comparado	695
11.1. Comisión de Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL)	695
11.2. Ley modelo de la CNUDMI sobre firmas electrónicas	696
11.3. Directiva 1999/93/CE de la Unión Europea.....	705
11.3.1. Requisitos de los certificados reconocidos	721
11.3.2. Requisitos de los proveedores de servicios de certificación que expiden certificados reconocidos	721
11.3.3. Requisitos de los dispositivos seguros de creación de firma electrónica.....	723
11.3.4. Recomendaciones para la verificación segura de firma	724
11.4. Normativa Comunitaria en el MERCOSUR	724
11.4.1. Resolución 34/06 GMC MERCOSUR.....	724
11.4.2. Estándares generales de interoperabilidad	726
11.4.3. Criterios de seguridad física y lógica de los prestadores de servicios de certificación	727
11.4.4. Criterios de auditoría y control de los prestadores de servicios de certificación	727
11.4.5. Criterios para la emisión de certificados reconocidos	728
11.4.6. Recomendación para la verificación segura de firma electrónica avanzada	728
11.5. Resolución 37/06 FMC Mercosur.....	729
11.6. Normas nacionales	736

	Pág.
11.6.1. Europa.....	736
11.6.2. Estados Unidos.....	738
11.6.3. América Latina	739
11.6.4. Oceanía	746
12. Reseña jurisprudencial	746
12.1. Ejecución hipotecaria y excepción de pago con comprobante de un cajero automático.....	746
12.2. Un "movimiento" en una base de datos de gestión judicial y la caducidad de instancia	748
12.3. Posibilidad de presentar escrito mediante comunicación electrónica.....	751
12.4. Una impresión no es un documento electrónico.....	751
12.5. No es válido un correo electrónico sin "firma digital"	752
12.6. Validez extracto cuenta bancaria en sede laboral.....	753
12.7. Recaudos en una pericia informática	753
12.8. Obtención de evidencia digital como diligencia preliminar.....	754
12.9. Admisibilidad del ofrecimiento de documentos electrónicos como prueba	754
12.10. Posibilidad de reconocimiento jurídico de las registraciones con tables electrónicas	755
12.11. Valoración de los medios digitales de almacenamiento de datos y diligencias necesarias para acceder a ellos.....	756
12.12. Requisitos que debe reunir el correo electrónico para ser admitido como prueba.....	756
13. Conclusiones	757
Bibliografía.....	758

CAPÍTULO IV

COMUNICACIONES ELECTRÓNICAS

1. Introducción	768
2. Comunicaciones electrónicas	772
2.1. Comunicaciones por computadoras.....	772
2.2. Correo electrónico (<i>e-mail</i>).....	775
2.2.1. Historia del correo electrónico	776
2.2.2. Cómo funciona el correo electrónico.....	778
2.2.3. Estructura de los mensajes de correo electrónico.....	785
3. Eficacia probatoria de los correos y comunicaciones electrónicas.....	788
3.1. Jurisprudencia argentina	792
3.2. Ley Modelo CNUDMI.....	803
3.3. Valor probatorio de las comunicaciones electrónicas según el derecho argentino.....	811
3.3.1. Telegramas.....	812

	Pág.
3.3.2. Cartas documento.....	813
3.3.3. Aplicación de estos criterios al correo electrónico.....	813
3.3.4. Los mensajes de correo electrónicos no firmados en las relaciones interempresarias.....	815
3.3.5. Aspectos técnicos a tener en cuenta.....	829
3.3.6. Aspectos importantes para una prueba pericial	834
3.3.7. Legislación española	847
3.4. Notificaciones electrónicas en Argentina	849
3.4.1. Documentos electrónicos	850
3.4.2. Firmas electrónicas y firmas digitales	853
3.4.3. Distintas acepciones de firma electrónica	856
3.4.4. Repercusión en el ámbito provincial.....	858
3.4.5. Consulta por Internet de expedientes judiciales.....	861
3.4.6. Antecedentes normativos	865
3.4.7. Reglamentación de la ley 26.685.....	870
3.4.8. Domicilios electrónicos constituidos.....	872
3.4.9. Experiencias latinoamericanas.....	876
3.4.10. Reglamentación del domicilio electrónico por la Corte Suprema.....	879
4. Confidencialidad de las comunicaciones electrónicas.....	890
4.1. La Directiva europea sobre protección de la intimidad en las comunicaciones electrónicas	893
4.2. Protección constitucional de la correspondencia en América Latina	910
4.3. La interceptación de las comunicaciones en la legislación argentina...	915
4.4. Intervención en las comunicaciones por orden judicial	918
4.5. El caso "Halabi".....	922
4.6. Interceptación de comunicaciones electrónicas de personas menores por parte de sus padres.....	924
5. Uso del correo electrónico y de las comunicaciones electrónicas en general, cuando han sido provistas por el empleador, en el ámbito laboral.....	928
5.1. Derecho comparado.....	929
5.1.1. Comunidad Europea	930
5.1.2. España.....	930
5.1.3. Portugal.....	937
5.1.4. Francia	938
5.1.5. Gran Bretaña	940
5.1.6. Alemania.....	940
5.1.7. Italia	941
5.1.8. Bélgica.....	941
5.1.9. Holanda	941
5.1.10. Estados Unidos de Norte América	941

	Pág.
5.2. América Latina	943
5.2.1. Brasil	943
5.2.3. Chile	944
5.3. Situación en la Argentina	945
5.4. Respuestas de la justicia laboral	947
5.4.1. Rechazo del despido	949
5.4.2. Justificación del despido	960
5.4.3. Nuestra posición	964
5.4.4. Situación en la Administración Pública Nacional.....	966
6. Aspectos jurídicos de comunicaciones electrónicas no deseadas	970
6.1. Qué es una comunicación electrónica no solicitada	970
6.2. Problemas que genera	972
6.3. Ilegalidad de los correos no deseados	974
6.4. El problema de la jurisdicción	977
6.5. La situación de las <i>cookies</i>	980
6.6. Marketing directo, intimidad y protección de datos personales....	981
6.7. Situación de los proveedores de servicios de Internet.....	986
6.8. Comunicaciones sindicales	995
6.9. Ley de Perú	998
Bibliografía	1002