



## ÍNDICE GENERAL

<b>CAPÍTULO I</b>	
<b>EL DERECHO A LA INTIMIDAD EN LAS COMUNICACIONES ELECTRÓNICAS, MENSAJES DE DATOS Y DE CUALQUIER OTRO TIPO</b>	
§ 1. Introducción	13
§ 2. El Reglamento Eprivacy de la UE y la confidencialidad de las comunicaciones electrónicas	14
§ 3. Antecedentes jurisprudenciales en instancias penal y civil sobre inviolabilidad de correspondencia electrónica	16
§ 4. Criterio de la «razonable expectativa de privacidad»	18
§ 5. Formas de vulnerar los correos electrónicos	19
§ 6. Métodos para preservar la intimidad en las comunicaciones electrónicas	21
a) El cifrado de los mensajes (criptografía)	21
b) Correo «web» cifrado	24
c) «Remailers»	25
d) «Darknet». Programas para ocultar IP	25
§ 7. Ley 26.388 y la violación de las comunicaciones electrónicas	25
— Crítica. Conveniencia de haber dispuesto la noción de «mensaje de datos»	26
§ 8. El Proyecto de Código Penal. Comisión Mariano Borinsky	28
<b>CAPÍTULO II</b>	
<b>EL DERECHO A LA INTIMIDAD FRENTE A LA VIGILANCIA Y MONITOREO PERSONAL</b>	
§ 9. Vigilancia y monitoreo de las personas	31
§ 10. Tecnologías de vigilancia y monitoreo	32
§ 11. Antecedentes normativos sobre vigilancia masiva estatal	36
a) Estados Unidos de América	36
1. «USA Patriot Act» (Acta Patriótica)	36
2. «The USA Freedom Act» (Ley de la Libertad de los Estados Unidos)	37
b) Reino Unido	37
c) Francia	38
d) Italia	39
§ 12. Programas estatales de vigilancia masiva	40
§ 13. Empresas privadas de videovigilancia y espionaje	41
§ 14. Documentos internacionales sobre la vigilancia	42
a) Conferencia de Juristas Nórdicos y la vigilancia (1967)	42
b) ONU	43
c) Resolución del Consejo de Derechos Humanos «El derecho a la privacidad en la era digital» de 2015	44
d) Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión e intimidad de las personas. ONU y OEA	44
e) La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos y los programas de recolección de metadatos telefónicos en los EE.UU. (mayo de 2015)	46
f) Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos sobre programas de vigilancia masiva (julio de 2015)	47
§ 15. Marcos normativos estrictos	48

<b>CAPÍTULO III</b>	
<b>EL EMPLEO DE PRÁCTICAS Y TECNOLOGÍAS INTRUSIVAS EN</b>	
<b>INVESTIGACIONES CRIMINALES COMPLEJAS. AFECTACIÓN A LA INTIMIDAD</b>	
§ 16. Introducción	49
§ 17. Interceptación y captura de comunicaciones telefónicas, electrónicas y de cualquier tipo	51
a) Introducción	51
b) Requisitos y principios	51
c) Normativa	54
1. Leyes de Telecomunicaciones, 27.078 "Argentina Digital" y 25.520 de Inteligencia Nacional. DNU 256/15y 102/17. Acordadas 2/16y 17/19 de la Corte Suprema de Justicia de la Nación	54
2. Código Procesal Penal de la Nación	61
3. Código Procesal Penal de la Provincia de Buenos Aires	61
4. Código Procesal Penal de la Provincia de Córdoba	62
5. Código Procesal Penal de la Provincia de Santa Fe	62
d) Antecedentes Jurisprudenciales	62
1. Intervenciones telefónicas y por Internet e intimidad. Corte Suprema de Justicia de la Nación. «Halabi»	62
2. Antecedente jurisprudencial de la Corte interamericana de Derechos Humanos sobre interceptación y monitoreo de comunicaciones. «Escher y otros v. Brasil»	64
§ 18. Interceptación y captura de comunicaciones electrónicas	66
a) Concepto de mensaje de datos	66
b) La cuestión de los datos de contenido y tráfico en las interceptaciones y captura de comunicaciones electrónicas	67
c) Los metadatos en las comunicaciones electrónicas y el Reglamento Eprivacy de la Unión Europea	68
d) Los datos de tráfico y contenido en el Convenio sobre la Cibercriminalidad de Budapest	70
e) Directivas europeas sobre comunicaciones electrónicas	70
1. Directiva 2002/58/CE o «Directiva sobre la privacidad y las comunicaciones electrónicas»	70
2. Directiva24/2006/CE del 15demarzode2006sobreiaconservaciónde datos generados o tratados en relación con la prestación deservicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones	71
3. Ley de Enjuiciamiento Criminal de España sobre interceptación de comunicaciones de los investigados (etapa previa) y encausado (tras el auto formal de acusación). Incorporación al proceso de datos electrónicos de tráfico o asociados	73
§ 19. Interceptaciones judiciales de correos electrónicos en el marco de investigaciones criminales	74
a) Antecedentes jurisprudenciales en la Argentina	74
b) La IP no se asimila a una interceptación de comunicaciones. Antecedente jurisprudencial del Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires. Investigación de un delito de pornografía infantil (art. 128.2, párr. 2°, CP)	80
c) Importante antecedente jurisprudencial. Informes sobre datos de las asignaciones de las direcciones IP y las celdas de conexión habilitadas con su correspondiente ubicación geográfica. Análisis sobre su validez. Afectación del derecho a la intimidad	81
§ 20. Identificación mediante la IP. Derecho comparado. Ley de Enjuiciamiento Criminal de España	85

§ 21. Programas informáticos espías en computadoras, dispositivos electrónicos, sistemas informáticos para investigaciones delictivas complejas	85
a) Requisitos para implantar programas espías con fines de investigación criminal	86
b) Registros remotos sobre equipos informáticos. Derecho comparado. Antecedente en la Ley de Enjuiciamiento Criminal de España	87
c) Dificultades que pueden preverse con la instrumentación de los programas espías dentro de una investigación criminal	90
§ 22. Monitoreo y ciberpatrullaje «online»	93
— Argentina	94
1. Antecedente jurisprudencial de ciberpatrullaje. «M. R. Damián y otros/intimidación pública»	94
2. Antecedentes normativos de ciberpatrullaje	94
I. Resolución 2018-31-APN-SECSEG MSG del 26 de julio de 2018. Secretaría de Seguridad	94
II. Resolución 144/2020-RESOL-2020-144-APN-MSG del 2 de junio de 2020. Ministerio de Seguridad	95
§ 23. Registro de los equipos informáticos	99
a) Peritaje sobre contenidos de teléfonos celulares solicitado por el fiscal sin orden de juez competente. Afectación del derecho a la intimidad. Antecedente «N.: J. O. s/Art. 91 CC»	101
b) Datos hallados en un teléfono celular extraviado. Quien lo encuentra revisa archivos (videos) y advierte posible comisión de ilícitos. Denuncia. Derecho a la intimidad. Antecedente jurisprudencial. CNCC, Sala de FERIA A, 15/1/15, «C. Q., Á. G. s/Nulidad»	102
c) Información almacenada en una computadora personal. Imágenes de pornografía infantil. Acceso de técnico informático en tareas de reparación y de la policía sin orden previa de juez competente. Antecedente jurisprudencial del Tribunal Europeo de Derechos Humanos, «Asunto Trabajo Rueda c. España»	103
d) Desbloqueo de teléfonos inteligentes. Antecedente jurisprudencial. EE. UU. Violación de la garantía de autoincriminación	105
§ 24. El empleo de GPS para el seguimiento policial en investigaciones criminales. Derecho a la intimidad	108
a) Geolocalización mediante telefonía móvil en investigaciones criminales. Antecedente «Carpenter» (EE. UU.). Repercusión jurisprudencial en nuestro país	112
b) Empleo de cámaras infrarrojas. Violación de domicilio e intimidad. Antecedente «Kyllo v. United States». Corte Suprema de los EE. UU.	115
c) El empleo de VANT/drones en investigaciones criminales. Invasión del espacio aéreo. Violación del domicilio y la intimidad. Antecedente «N. N. s/Estupefacientes -siembra o cultivo- artículo 5 Ley 23.737»	116
§ 25. Tratamiento de datos por organismos de seguridad e inteligencia en el proyecto de Ley de Protección de Datos Personales de Argentina	117
§ 26. Investigación de delitos complejos mediante técnicas intrusivas: ¿El principio de sospecha por el principio de inocencia?	118
§ 27. Estado de derecho e investigaciones criminales complejas. Necesidad de un marco normativo acorde	119
<b>CAPÍTULO IV</b>	
<b>VIDEOVIGILANCIA</b>	
§ 28. Introducción	123
§ 29. Videovigilancia. Finalidades	124
§ 30. Derecho a la intimidad, imagen y videovigilancia	126
§ 31. Seguridad e intimidad	127
§ 32. La imagen como dato y la videovigilancia	131
§ 33. Resolución 4/19 de la Agencia de Acceso a la Información Pública. Derecho de Acceso a datos personales recolectados mediante sistema de videovigilancia	132

§ 34. Biometría. Entrecruzamiento de datos personales. El Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS). Decreto 1766/11	133
§ 35. Videovigilancia en espacios públicos. Regulación normativa. Antecedentes	135
§ 36. Antecedentes nacionales	141
a) Resolución 283/12 del Ministerio de Seguridad de la Nación	142
b) Disposición 10/15 de la Dirección Nacional de Protección de Datos Personales (DNPDP)	143
c) Antecedentes legislativos provinciales	145
1. Ciudad Autónoma de Buenos Aires. Ley 2602	145
2. Sistema Integral de Seguridad Pública de la Ciudad Autónoma Buenos Aires. Ley 5688	148
3. Provincia de Córdoba. Ley 9380	150
§ 37. Sistemas privados de videovigilancia	151
§ 38. La videovigilancia en entradas a edificios y el derecho a la intimidad — Antecedente legislativo. Sistemas privados de videovigilancia. Ciudad Autónoma de Buenos Aires. Ley 5688/16	153
§ 39. Cámaras de videovigilancia falsas. Afectación de la intimidad. Interesante antecedente español	155
§ 40. Cámaras IP para vigilancia privada y la intimidad	156
§ 41. Instalación de cámara de videovigilancia en establecimientos educativos	157
a) España	157
b) Argentina. Antecedentes jurisprudenciales	158
§ 42. Instalación de cámaras en Centro de identificación y Alojamiento Provisorio de Niños, Niñas y Adolescentes (Ciudad Autónoma de Buenos Aires). Derecho a la intimidad. Antecedente jurisprudencial: Causa n° 15363/2017, «Asesoría Tutelar n° 1 s/Hábeas corpus». Apelación	159
§ 43. El empleo de drones para videovigilancia en espacios públicos y el derecho a la imagen e intimidad — Disposición 20/15 de la Dirección Nacional de Protección de Datos Personales (DNPDP)	161
§ 44. Efectos de la videovigilancia sobre las personas	163
§ 45. Desvíos de fines en la videovigilancia	164
§ 46. Videovigilancia y la autodeterminación informática	165
§ 47. Resolución 4/2019 de la Agencia de Acceso a la Información Pública. Derecho de Acceso a datos personales recolectados mediante sistema de videovigilancia	165
§ 48. Conclusión sobre la videovigilancia	166

## CAPÍTULO V

### **MONITOREO EN LAS RELACIONES LABORALES. COMUNICACIONES ELECTRÓNICAS EN EL ÁMBITO LABORAL**

§ 49. El monitoreo laboral de las comunicaciones electrónicas. Nociones generales. Afectación al derecho de intimidad. Discusiones doctrinarias. Jurisprudencia nacional y extranjera	169
§ 50. Normativa en el derecho extranjero acerca del monitoreo laboral del correo electrónico	177
§ 51. Situación en la Argentina. El correo electrónico laboral. Información previa de la política empresarial en cuanto al empleo del correo electrónico. Jurisprudencia	179
§ 52. Documentos que avalan el monitoreo	181
§ 53. Antecedentes jurisprudenciales a favor del trabajador por no existir información ni documento previo	182
§ 54. La casilla de correo electrónico privado del trabajador y la posibilidad de control	184
§ 55. Empleo de teléfonos inteligentes y aplicaciones de mensajería instantánea como herramientas laborales	185
§ 56. Antecedente europeo sobre control de mensajes instantáneos laborales	185

§ 57. Empleo de mensajería instantánea en teléfono inteligente propiedad del empleado	186
§ 58. «Chat». Antecedentes jurisprudenciales	186
a) Argentina	186
b) España	187
§ 59. Acceso indebido a la correspondencia electrónica del trabajador	188
§ 60. Indagar datos y perfiles personales en Internet que puedan condicionar el acceso a un trabajo. Interesante antecedente en nuestro país. Amparo de la Unión de Trabajadores de la Educación contra el Gobierno de la Ciudad Autónoma de Buenos Aires	188
§ 61. Videovigilancia y tecnologías de monitoreo laboral	189
a) Introducción	189
b) Requisitos para presentar las filmaciones como prueba en materia de despidos	190
c) Antecedentes jurisprudenciales en Argentina	190
1. Videovigilancia laboral. Intimidación	190
2. Despido. Prueba del despido. Cámaras de video	191
I. «Figuroa, Sergio c. Cía. de Servicios Hoteleros S.A. s/Despido»	191
II. «Montero, Alejandro Oseare. Swiss Medical S.A. s/Despido»	191
III. Otros precedentes	192
d) La protección de datos en España	193
1. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	193
2. Antecedentes jurisprudenciales	195
§ 62. El GPS como herramienta de control laboral	196
— Antecedentes jurisprudenciales	197
1. Argentina. «Pavolotzki, Claudio y otros c. Fischer Argentina S.A. s/Sumarísimo»	197
2. España	199
§ 63. Empleo de «chips» RFDI para monitoreo laboral	200
§ 64. Empleo de tecnologías biométricas para control en el ámbito laboral	201
§ 65. Pulseras para monitoreo laboral	202
§ 66. Recomendación CM/Rec (2015)5 del Comité de Ministros a los Estados miembros sobre el tratamiento de datos personales en el contexto del empleo	202
§ 67. Teletrabajo. Control. Prohibición, «software» de vigilancia. Derecho a la intimidad. Ley 27.555. Decreto reglamentario 27/2021	206
a) Teletrabajo. Control. Derecho a la intimidad. Ley 27.555. Decreto reglamentario 27/2021	206
— Antecedente normativo	207
I. Chile	207
II. Argentina. Ley 27.555	208
<b>BIBLIOGRAFÍA GENERAL</b>	211