EL PRINCIPIO DE SEGURIDAD JURIDICA EN EL MUNDO VIRTUAL

CARLOS E. DELPIAZZO
Profesor de Derecho Administrativo, Profesor de Informática Jurídica
y Director del Instituto de Derecho Informático (U de la R)
Profesor de Derecho Administrativo, Director del Programa Master de Derecho
Administrativo Económico (PMDAE)
y Profesor de Derecho Informático (UM)

SUMARIO:

I. BASE CONSTITUCIONAL

La primera de las disposiciones de la Sección II de nuestra Constitución, titulada «Derechos, deberes y garantías», prevé que «Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, *seguridad*, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecieren por razones de interés general» (art. 7º).

Según lo destacara el máximo comentarista de nuestra Carta constitucional, «El derecho a la protección de la seguridad es un concepto muy amplio, que abarca el derecho a ser amparado por todas las normas de garantía relativas a los demás derechos constitucionalmente consagrados, y por las disposiciones legales que se dicten con la misma finalidad, en ejecución de los mandatos del constituyente» [(1)].

Más adelante, la Constitución particulariza respecto a distintos aspectos de la seguridad.

Así, el art. 31 prevé que "La *seguridad individual* no podrá suspenderse sino con la anuencia de la Asamblea General, o estando ésta disuelta o en receso, de la Comisión Permanente, y en el caso extraordinario de traición o conspiración contra la patria".

A su vez, el art. 168, num. 1º dispone que al Poder Ejecutivo corresponde "La conservación del orden y tranquilidad en lo interior, y la *seguridad en lo exterior*".

Por su parte, el art. 195 crea el Banco de Previsión Social "con el cometido de coordinar los servicios estatales de previsión social y organizar la *seguridad social*".

Finalmente, el art. 262 establece que "El gobierno y la administración de los Departamentos, con excepción de los servicios de *seguridad pública*, serán ejercidos por una Junta Departamental y un Intendente".

De este modo, dentro del género seguridad, la Constitución refiere a especies tales como la seguridad individual, la seguridad en lo exterior, la seguridad social y la seguridad pública.

II. NOCION

Respecto a la noción de **seguridad**, cabe decir que "Es un sustantivo que traduce un estado institucional y/o personal. Proviene del latín securitas que dice de sus propiedades o de los componentes de lo propio, en tanto se refiere a lo cierto, lo confiable, lo indemne, lo conocido, lo indubitable, lo responsable, lo sólido, lo

1. Justino JIMENEZ DE ARECHAGA - «La Constitución Nacional» (Cámara de Senadores, Montevideo, 1991), tomo I, pág. 340.

infalible, lo estable, lo continuo, lo transparente, lo tranquilo, lo protegido, lo amparado, de y en la vivencia y la convivencia» [2].

La misma se traduce "como la certidumbre del individuo de que su persona, bienes y derechos están a salvo de ataques violentos e indebidos y, en el peor de los casos, de efectuarse, se harán cesar con premura y los daños le serán resarcidos; la seguridad es, por tanto, punto de partida del Estado y puerto de arribo del derecho" [3].

Apreciada en sus caracteres, la seguridad como indicativa de la calidad de seguro, es decir, libre y exento de todo peligro, daño o riesgo, busca la salvaguarda de la unicidad de la persona humana, es reclamo de su dignidad inherente, y no halla su razón de ser en el Estado ni en la sociedad sino en el hombre como fin [4].

Dentro de tal concepto genérico de seguridad, es posible distinguir distintas especies o clases [5], tales como:

a) la seguridad jurídica;
b) la seguridad pública [6] o ciudadana [7] como integrante del concepto de orden público;
c) seguridad individual o humana [8];
d) seguridad social [9]; y
e) seguridad nacional [10].

En cuanto a la **seguridad jurídica**, la misma alude a la certeza, el orden, la firmeza y la confianza en el ordenamiento [11], no sólo en las relaciones jurídicas entre particulares sino especialmente en las relaciones entre el ciudadano y la Administración y aún frente al legislador [12].

Según se ha dicho, la seguridad jurídica tiene un componente objetivo fincado en la certeza de la positividad del Derecho y su observancia, y en su aspecto subjetivo tiene en cuenta la confianza puesta por la persona en el comportamiento correcto de quienes deben aplicarlo [13].

III) NATURALEZA JURIDICA

Prescindiendo de la discusión -más bien filosófica- acerca de si la seguridad jurídica es un valor o un principio [14], desde el punto de vista jurídico tiene la operatividad de un principio porque es en sí lo primero [15].

En orden a su **caracterización**, es posible hacer coincidir la definición de los principios generales de Derecho con su designación, a través de las tres palabras que componen su nombre [16].

2. Luciano PAREJO ALFONSO y Roberto DROMI - «Seguridad pública y Derecho administrativo» (E.C.A. - Marcial Pons, Buenos Aires - Madrid, 2001), pág. 201.
3. Jorge FERNANDEZ RUIZ - "Apuntes para una teoría jurídica de la seguridad", en Anuario de Derecho Administrativo, tomo X, pág. 39.
4. Mariano R. BRITO - "Seguridad. Visión desde una óptica unitaria", en Jorge FERNANDEZ RUIZ (Coordinador) - "Derecho Administrativo. Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados" (UNAM, México, 2005), pág. 591 y sigtes.
5. Carlos E. DELPIAZZO - "Derecho Administrativo Especial" (A.M.F., Montevideo, 2006), volumen I, pág. 290 y sigtes.
6. Gabino E. CASTREJON GARCIA - "La seguridad pública en el marco administrativo y constitucional", en Jorge FERNANDEZ RUIZ (Coordinador) - "Derecho Administrativo. Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados" (UNAM, México, 2005), pág. 601 y sigtes.
7. Luciano PAREJO ALFONSO - "La seguridad ciudadana y el orden público", en Luciano PAREJO ALFONSO y Roberto DROMI - «Seguridad pública y Derecho administrativo» (E.C.A. - Marcial Pons, Buenos Aires - Madrid, 2001), pág. 44.
8. Graciela LOPEZ MACHIN - "La seguridad humana como garantía de la persona", en Rev. de Derecho Público, Año 2003, Nº 24, pág. 155 y sigtes.
9. Julio A. PRAT - "Seguridad social y Acto Institucional Nº 9" (A.M.F., Montevideo, 1980), pág. 9 y sigtes.; y Américo PLA RODRIGUEZ - "Introducción y conceptos generales", en A.A.V.V. - "La seguridad social en el Uruguay" (F.C.U., Montevideo, s/f), pág. 17 y sigtes.
10. Mariano R. BRITO - «Defensa nacional», en Introducción al estudio actualizado de los cometidos estatales (F.C.U., Montevideo, 2000), pág. 89 y sigtes.
11. Federico A. CASTILLO BLANCO - "El principio de seguridad jurídica: especial referencia a la certeza en la creación del Derecho", en Documentación Administrativa (INAP, Madrid, 2002), Nº 263-264, pág. 33.
12. Trabajos varios en Documentación Administrativa (INAP, Madrid, 2002), Nº 263-264.
13. Pedro José Jorge COVIELLO - "La confianza legítima", en VII Jornadas Internacionales de Derecho Administrativo Allan R. Brewer Carías (FUNEDA, Caracas, 2004), tomo I, pág. 295 y sigtes.; y "La protección de la confianza del administrado" (Lexis Nexis, Buenos Aires, 2004), pág. 293 y sigtes.
14. Federico A. CASTILLO BLANCO - "El principio de seguridad jurídica: especial referencia a la certeza en la creación del Derecho" cit., pág. 36 y sigtes.
15. José Aníbal CAGNONI - "La primacía de la persona: el principio personalista", en Rev. de Derecho Público (Montevideo, 2003), Nº 24, pág. 135 y sigtes.
16. Carlos E. DELPIAZZO - "Derecho Administrativo Uruguayo" (UNAM - Porrúa, México, 2005), págs. 12 y 13.

En primer lugar, son principios por cuanto constituyen los soportes primarios estructurales del sistema jurídico todo, al que prestan su contenido. Como bien lo ha destacado REAL, «en todo sistema jurídico hay cantidad de reglas de gran generalidad, verdaderamente fundamentales, en el sentido de que a ellas pueden vincularse, de un modo directo o indirecto, una serie de soluciones expresas del Derecho positivo a la vez que pueden resolverse, mediante su aplicación, casos no previstos, que dichas normas regulan implícitamente» [17]. Se trata de auténticos cimientos que cumplen la triple función de servir como criterio de interpretación de las normas escritas, de colmar las lagunas o vacíos normativos, y de constituir el medio más idóneo para asegurar la unidad dentro de la pluralidad de preceptos que se aplican en la Administración [18].

En segundo lugar, son reglas de carácter general porque trascienden un precepto concreto y no se confunden con apreciaciones singulares o particulares.

En tercer lugar, los principios generales son de Derecho ya que se trata de fórmulas técnicas del mundo jurídico y no de simples criterios morales, buenas intenciones o vagas directivas. A pesar de que no se presentan habitualmente con la estructura típica de una regla de Derecho, ninguna duda puede existir acerca de que revisten el carácter de tal [19].

Desde el punto de vista de su **jerarquía**, participan de la suprema eficacia normativa de la Constitución e, incluso, para parte de la doctrina, se ubican por encima de la misma por ser anteriores a ella, que los reconoce nominadamente en el art. 332 e innominadamente en el art. 72, a cuyo tenor "La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o que se derivan de la forma republicana de gobierno". Quiere decir que derechos o deberes y garantías inherentes a la personalidad humana o que derivan de la forma republicana de gobierno, no enumerados por la Constitución, integran el concepto de "regla de Derecho" según lo explicita el art. 23, lit. a) del decreto ley orgánico del Tribunal de lo Contencioso Administrativo Nº 15.524 de 9 de enero de 1984 al disponer que se considera tal "todo principio de Derecho o norma constitucional, legislativa, reglamentaria o contractual".

Además, según lo destacara BARBE PEREZ, constituyen fuente directa y principal de nuestro Derecho porque "sería ontológicamente absurdo y lógicamente contradictorio que siendo principios generales sólo se apliquen si no hay texto, sino que los textos deben estar de acuerdo a los principios y los principios de acuerdo a la naturaleza de las cosas" [20].

Si en todos los campos del Derecho la **importancia** de los principios generales de Derecho es cardinal, ello es especialmente cierto en el ámbito de un Derecho novedoso, como es el Derecho Telemático, con vocación de universalidad y en formación requerido de piezas arquitecturales del ordenamiento, cuya manifestación se verifica fundamentalmente a través de la práctica aplicativa del Derecho y del desarrollo de la ciencia jurídica [21].

IV) SEGURIDAD EN EL MUNDO VIRTUAL

Parece obvio que la seguridad en el mundo virtual (intrínsecamente intangible) no puede lograrse del mismo modo y a través de los mismos instrumentos que la seguridad proveniente del mundo preinformático (sustentado en lo tangible), adquiriendo nuevas tonalidades a la luz de la novedosa realidad [22].

Especialmente, en los negocios, la forma exigida para los contratos, la registración pública, la certificación de las firmas y otros institutos no son medios de seguridad apropiados cuando los contratos se celebran a distancia, entre ausentes, sin escritos y hasta en forma anónima [23].

17. Alberto Ramón REAL - «Los principios generales de Derecho en la Constitución uruguaya» (Montevideo, 1965), pág. 16, y en A.A.V.V. - "Los principios generales de Derecho en el Derecho uruguayo y comparado" (F.C.U., Montevideo, 2001), pág. 87 y sigtes.
18. Héctor FRUGONE SCHIAVONE - «Principios del procedimiento administrativo», en A.A.V.V. - "El nuevo procedimiento administrativo" (Pronade, Montevideo, 1991), págs. 31 y 40.
19. Juan Pablo CAJARVILLE PELUFFO - «Reflexiones sobre los principios generales de Derecho en la Constitución uruguaya», en Estudios Jurídicos en memoria de Alberto Ramón Real (F.C.U., Montevideo, 1996), pág. 173 y sigtes., y en A.A.V.V. - "Los principios generales de Derecho en el Derecho uruguayo y comparado" cit., pág. 137 y sigtes.
20. Héctor BARBE PEREZ - «Los principios generales de Derecho como fuente de Derecho administrativo en el Derecho positivo uruguayo», en Estudios Jurídicos en memoria de Juan José Amézaga (Montevideo, 1958), pág. 37 y sigtes., y en A.A.V.V. - "Los principios generales de Derecho en el Derecho uruguayo y comparado" cit., pág. 19 y sigtes.
21. Carlos E. DELPIAZZO y María José VIEGA - "Lecciones de Derecho Telemático" (F.C.U., Montevideo, 2004), pág. 73 y sigtes.
22. Carlos E. DELPIAZZO - "¿Hacia dónde va el Derecho de Internet?", en Derecho Informático (F.C.U., Montevideo, 2004), tomo IV, pág. 247 y sigtes.
23. Michael BEXKER - «Las transacciones electrónicas y sus influencias en el Derecho civil y administrativo y la posición de los notarios alemanes y holandeses», en A.A.V.V. - «La seguridad jurídica en las transacciones electrónicas» (Civitas, Madrid, 2002), pág. 63 y sigtes.

Según se ha destacado con acierto, «Durante las primeras décadas de su existencia, las redes de computadoras fueron usadas principalmente por investigadores universitarios para el envío de correo electrónico, y por empleados corporativos para compartir impresoras. En estas condiciones, la seguridad no recibió mucha atención. Pero ahora, cuando millones de ciudadanos comunes usan redes para sus transacciones bancarias, compras y declaraciones de impuestos, la seguridad de las redes aparece en el horizonte como un problema potencial de grandes proporciones... Los problemas de seguridad de las redes pueden dividirse en términos generales en cuatro áreas interrelacionadas: secreto, validación de identificación, no repudio y control de integridad. El *secreto* tiene que ver con mantener la información fuera de las manos de usuarios no autorizados. Esto es lo que normalmente viene a la mente cuando la gente piensa en la seguridad de las redes. La *validación de identificación* se encarga de determinar con quién se está hablando antes de revelar información delicada o hacer un trato de negocios. El *no repudio* se encarga de de las firmas... Por último, ¿cómo puede asegurarse de que un mensaje recibido realmente fue el enviado, y no algo que un adversario malicioso modificó en el camino o cocinó por su propia cuenta?» [(24)], es decir, que no fue alterado en su *integridad*.

Para atender a los cuatro aspectos de seguridad indicados, deben adoptarse previsiones tanto en el hardware como en el software de red y, especialmente, en la llamada capa de aplicación, en la cual se implementarán soluciones de cifrado. El arte de diseñar cifradores (criptografía) y de descifrarlos (criptoanálisis) se conocen colectivamente como criptología.

Según se ha destacado, «La criptografía moderna usa las mismas ideas básicas que la criptografía tradicional, la transposición y la sustitución, pero su orientación es distinta. Tradicionalmente, los criptógrafos han usado algoritmos sencillos y se han apoyado en claves muy largas para la seguridad. Hoy día es cierto lo inverso: el objetivo es hacer el algoritmo de cifrado tan complicado y rebuscado que inclusive si el criptoanalista obtiene cantidades enormes de texto cifrado a su gusto, no será capaz de entender nada» [(25)].

Además, a partir de 1976, el sistema clásico de algoritmo de clave secreta, vino a ser superado por el algoritmo de clave pública, en el que las claves de cifrado y descifrado son diferentes, posibilitando formas más sofisticadas de aseguramiento [(26)].

En síntesis, es evidente que la seguridad jurídica reclama siempre y en todo caso -también en Internet- certeza, estabilidad y razonabilidad, a cuyo alcance deben converger tanto soluciones normativas como tecnológicas.

V) SEGURIDAD DE LA INTIMIDAD

Capítulo aparte merece la consideración de la seguridad -especialmente en el primero de los aspectos antes señalados- en su relación con el derecho a la intimidad -y su nuevo rostro actual: el derecho a la protección de los datos personales [(27)]- en el mundo globalizado a través de las telecomunicaciones [(28)].

A) Perspectiva

En varias oportunidades anteriores [(29)], he recordado que «Todo ser humano guarda siempre un misterio en su corazón, una zona reservada a la mirada indiscreta de cualquier otro, que constituye el núcleo más hondo y arraigado de su personalidad, aquello que le hace sentirse autónomo y diferente. Se trata de todo ese mundo interior donde anidan y se esconden los sentimientos, deseos, ilusiones, pensamientos, alegrías y penas, nostalgias o vergüenzas, experiencias e historias, acontecimientos y omisiones..., que son nuestro patrimonio más auténtico, lo único que nos pertenece por completo, porque nos hace sentirnos como sujetos personales, no como un objeto cualquiera expuesto a la contemplación curiosa de los demás» [(30)].

24. Andrew S. TANENBAUM - «Redes de Computadoras» (Pearson, México, 1997), 3ª edición, pág. 577 y sigtes.
25. Andrew S. TANENBAUM - «Redes de Computadoras» cit., pág. 587 y sigtes.
26. Carlos E. DELPIAZZO - «La autenticación de las operaciones comerciales en Internet», en anuario Derecho Informático» (F.C.U., Montevideo, 2001), tomo I, pág. 256.
27. Carlos E. DELPIAZZO - «Protección de los datos personales en tiempos de Internet. El nuevo rostro del derecho a la intimidad», en Rev. de Derecho de la Universidad Católica del Uruguay (Montevideo, 2002), Nº III, pág. 253 y sigtes.
28. Carlos E. DELPIAZZO - "Derecho de las Telecomunicaciones" (U.M., Montevideo, 2005), pág. 87 y sigtes.
29. Carlos E. DELPIAZZO - «Dignidad humana y Derecho» (U.M., Montevideo, 2001), pág. 123 y sigtes.; y "El derecho a la intimidad en el ciberespacio", en Anales de las 30 Jornadas Argentinas de Informática e Investigación Operativa (Buenos Aires, 2001), pág. 51 y sigtes.
30. Eduardo LOPEZ AZPITARTE - "Etica y vida" (Edic. Paulinas, Madrid, 1990), pág. 330.

El reconocimiento explícito de este derecho es relativamente reciente y muestra una evolución que puede examinarse a través de ciclos sucesivos, sentidos diferentes y enfoques diversos, en cuyo marco procede ubicar la protección jurídica actual de los datos personales en general y en el sector de las telecomunicaciones en particular.

En cuanto a la evolución histórica del derecho a la intimidad, es habitual señalar como hito fundamental en su perfilamiento, el clásico «right to be alone» (1890), es decir, el derecho a ser dejado sólo o a ser dejado en paz o a no ser importunado. Este concepto de «privacy» apuntó básicamente a una protección jurídica contra la publicidad de actos o datos personales puestos en conocimiento del público sin noticia o permiso de la persona afectada. Posteriormente, dicho concepto se extendió para abarcar el derecho de los individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y con qué extensión puede ser comunicada a terceros la información acerca de aquéllos.

En cuanto al sentido de este derecho, el mismo ha transitado desde un sentido negativo (meramente garantista) hacia un sentido positivo. Al respecto, se ha señalado que hasta la consolidación de la sociedad industrial, el «right to privacy» constreñía su contenido al conjunto de facultades de exclusión de ingerencias de terceros en la esfera íntima. En cambio, a partir de la segunda mitad del siglo XX comienza a adquirir un sentido positivo, en la medida que ya no sólo se trata de establecer barreras para preservar la integridad de la dimensión interior del individuo sino que además se afirma la «privacy» como un presupuesto del ejercicio de otros derechos con proyección social e incluso económica.

En cuanto al modo de encarar la protección de la intimidad, se advierte que originalmente el diseño de su tutela se fundó en el concepto de propiedad, extendiendo como medios de protección las herramientas jurídicas pensadas para la tutela del dominio. Ello ha permitido hablar de una visión «patrimonialista» de Derecho privado, luego superada por un enfoque desde la perspectiva del Derecho público que pone el acento en la eminente dignidad humana y en la protección de sus derechos fundamentales [(31)].

La irrupción de la Informática primero [(32)] y de la Telemática después, como resultante de su encuentro con las Telecomunicaciones [(33)], ha replanteado la cuestión del derecho a la intimidad en atención al riesgo que para la persona implica la estructuración de grandes bancos de datos de carácter personal, y particularmente la potencialidad del entrecruzamiento de información contenida en ellos.

A partir de esa realidad, «*la libertad informática*" [(34)] aparece como un nuevo derecho de autotutela de la propia identidad informática, o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico.

Frente al «poder informático» de quienes pueden acumular informaciones sobre cada persona en cantidad ilimitada, de memorizarla, usarla y transferirla como una mercancía, el derecho a la intimidad se configura como una nueva forma de libertad personal, ya no caracterizada negativamente como la posibilidad de refutar o evitar el uso de datos referidos a cada uno, sino positivamente como la potestad de ejercer un poder de control sobre las informaciones referidas a la propia persona. Consiste en lo que ha dado en llamarse libertad informática, consistente en el derecho de autotutela de la propia identidad informática, es decir, en el derecho de vigilar los datos personales incluidos en archivos automatizados.

Frente a las posibilidades tecnológicas de conseguir un «ciudadano de cristal», la libertad informática es el derecho de disponer de la información personal, de preservar la propia identidad informática o, lo que es lo mismo, de consentir, controlar y rectificar los datos informativos concernientes a la propia personalidad; al derecho de informar y de ser informado se ha agregado el derecho de proteger la libertad de la información como un bien personal, que constituye un nuevo derecho fundamental, propio de la tercera generación, que tiene por finalidad el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente.

31. Héctor GROS ESPIELL - "La dignidad humana en los instrumentos internacionales de derechos humanos", en CATEDRA UNESCO DE DERECHOS HUMANOS - "Dignidad Humana" (Universidad de la República, Montevideo, 2003), pág. 9 y sigtes.; y José Aníbal CAGNONI - "La dignidad humana. Naturaleza y alcances", en CATEDRA UNESCO DE DERECHOS HUMANOS - "Dignidad Humana" cit., pág. 65 y sigtes., y en Rev. de Derecho Público, Año 2003, Nº 23, pág. 11 y sigtes.
32. Carlos E. DELPIAZZO - «Información, Informática y Derecho» (A.M.F., Montevideo, 1989), pág. 67 y sigtes.
33. Carlos E. DELPIAZZO - "Derecho de la Informática y las Telecomunicaciones", en XXIX Curso de Derecho Internacional (O.E.A., Washington, 2002), pág. 395 y sigtes.; «El Derecho telemático: respuesta a la convergencia tecnológica», en VII Congreso Iberoamericano de Derecho e Informática (Lima, 2000), pág. 54 y sigtes.; «El Derecho ante las telecomunicaciones, la informática e Internet», en anuario "Derecho Informático" (F.C.U., Montevideo, 2003), tomo III, pág. 41 y sigtes.; y Carlos E. DELPIAZZO y María José VIEGA - "Lecciones de Derecho Telemático" cit., pág. 51 y sigtes.
34. Carlos E. DELPIAZZO - «Poder y libertad informática», en Rev. Sistemas de Informática (Montevideo, 1985), págs. 16 y 17; y «Nuevamente sobre poder y libertad informáticos», en Primeras Jornadas Nacionales de Derecho Informático (Montevideo, 1987), pág. 147 y sigtes.

Teniendo en cuenta esta realidad, la doctrina y jurisprudencia alemanas han preferido hablar del «*derecho a la autodeterminación informativa*» [35] a partir del sonado caso resuelto por el Tribunal Constitucional en la sentencia de 15 de diciembre de 1983, en la cual se examinó la constitucionalidad de la ley de censo de población, concluyéndose que no sería compatible con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciesen posible «el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo se sabe algo sobre él... La libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a su persona».

Finalmente, cabe destacar que un sector de la doctrina utiliza la expresión «*derecho a la protección de datos personales*» [36] para designar el derecho bajo examen cuyo objeto es la tutela de una parte sustancial del derecho a la intimidad: la que se refiere a la información individual.

Es que hoy resulta extraordinariamente sencillo acceder a datos personales con el nombre, apellidos, domicilio, teléfono, fax, dirección de correo electrónico u otros que, pudiendo parecer inocuos, al cruzarlos con los hábitos de consumo o al tratarlos con programas datamining -dedicados a buscar información sensible escondida dentro de bases de datos- nos proporcionan, al entrecruzarse como haces de luz, una silueta virtual perfecta que refleja el yo más íntimo del potencial usuario o consumidor, perfecta representación de sus tendencias naturales, intuitivas e instintivas.

Muchas veces, los datos personales son facilitados voluntariamente por el propio titular de los mismos para acceder gratuitamente a algún servicio o para la obtención onerosa de un bien a través de Internet sin tener conciencia de que los mismos pueden ser utilizados para fines diferentes de aquellos para los que fueron recabados. Pero otras veces los datos del internauta son dejados por éste de manera completamente involuntaria ya que, una vez que los mismos salen de su computador, desconoce la ruta que siguen hacia su destino, en qué puntos intermedios se almacenan temporalmente y quién puede acceder a ellos, copiarlos, modificarlos y utilizarlos para cualquier finalidad diferente de aquélla para la que fueron entregados.

Según se ha destacado con acierto [37], los servicios de telecomunicaciones constituyen un ámbito específico y peculiar para la protección de los datos personales por dos razones principales: por un lado, porque las crecientes interoperatividad y extensión de estos servicios constituyen por sí mismas un factor de riesgo para la seguridad de la gestión de la información en general y de los datos relacionados con la intimidad en particular; y por otro lado, porque el proceso de telecomunicación requiere determinar e identificar los puntos de terminación de la red entre los que se produce la comunicación, puntos que por su eventual identificación con personas, pueden alcanzar la consideración de datos personales.

En ese contexto, cabe referirse al tratamiento jurídico que el tema viene mereciendo a nivel comparado y en nuestro país, con especial referencia al ámbito de las telecomunicaciones.

B) Panorama comparado

En el marco de la evolución regulatoria de la seguridad de los datos personales [38], los últimos años muestran a nivel del **Derecho internacional** una creciente concientización por el tema, centrada en el amparo debido a las personas contra la posible utilización por terceros, en forma no autorizada, de sus datos personales para confeccionar con ellos informaciones que afecten o puedan afectar su entorno personal, profesional o social, en los límites de su intimidad.

35. Erhard DENNINGER - «El derecho a la autodeterminación informativa», en A.A.V.V. - «Problemas actuales de la documentación y la informática jurídica» (Tecnos, Madrid, 1987), pág. 268 y sigtes.; Winfried HASSEMER y Alfredo CHIRINO SANCHEZ - «El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales» (Edit. del Puerto, Buenos Aires, 1997), pág. 166 y sigtes.; y Pablo Lucas MURILLO DE LA CUEVA - «El derecho a la autodeterminación informativa» (Tecnos, Madrid, 1990).
36. Miguel Angel EKMEKDJIAN y Calogero PIZZOLO - "Habeas data. El derecho a la intimidad frente a la revolución informática" (Depalma, Buenos Aires, 1996), pág. 5 y sigtes.; Julio TELLEZ VALDES - "Derecho Informático" (Mc Graw Hill, México, 2004), 3ª edición, pág. 57 y sigtes.; Miguel Angel DAVARA RODRIGUEZ - "Manual de Derecho Informático" (Thomson - Aranzadi, Navarra, 2004), 6ª edición, pág. 43 y sigtes.; Alfonso ORTEGA GIMENEZ - "El derecho a la protección de datos de carácter personal en Internet", en X Congreso Iberoamericano de Derecho e Informática (Santiago de Chile, 2004), pág. 223 y sigtes.; y Alvaro CANALES GIL - "La protección de datos personales como derecho fundamental", en anuario "Derecho Informático" (F.C.U., Montevideo, 2004), tomo IV, pág. 261 y sigtes.
37. Agustín DE ASIS ROIG - "Protección de datos y Derecho de las telecomunicaciones", en A.A.V.V. - "Régimen jurídico de Internet" (La Ley Actualidad, Madrid, 2002), págs. 201 a 203.
38. Carlos E. DELPIAZZO y María José VIEGA - "Lecciones de Derecho Telemático" cit., pág. 227 y sigtes.

Especialmente a nivel europeo, cabe señalar en primer lugar como antecedente relevante en la materia, el Convenio Nº 108 del Consejo de Europa sobre protección de las personas con relación al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981, conocido como Convenio de Estraburgo y abierto a la adhesión de Estados no miembros del Consejo de Europa [39].

Conforme al mismo, se procura «garantizar, en el territorio de cada Parte, a toda persona física, cualesquiera que fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales y en especial de su derecho a la intimidad con respecto al tratamiento automático de los datos de carácter personal que le conciernen» (art. 1). Para ello, establece una serie de principios relativos a los datos personales y a los ficheros computarizados (art. 5 y sigtes.), a la vez que define un «núcleo irreductible» (y no una lista exhaustiva) de datos sensibles, cuales son los que «revelaren el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual» (art. 6).

En segundo lugar, corresponde hacer referencia a la Directiva del Parlamento Europeo y del Consejo Nº 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos [40].

De acuerdo a esta Directiva también se consagran una serie de principios relativos a la calidad de los datos y el tratamiento de los mismos, se regulan los datos sensibles bajo el rótulo de «categorías especiales de tratamientos», se jerarquiza el consentimiento del afectado, se establece la obligación de informar al interesado, se reconoce ampliamente y se garantiza el derecho de acceso, se regula la confidencialidad y seguridad del tratamiento de los datos de carácter personal, y se promueve la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales en el marco de la Directiva.

En tercer lugar, ya con específica referencia al campo de las telecomunicaciones, es preciso mencionar la Directiva del Parlamento Europeo y del Consejo Nº 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones [41].

De acuerdo a la misma, "El proveedor de un servicio público de telecomunicación deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de telecomunicación por lo que respecta a la seguridad de la red" (art. 4º). Cabe aclarar que el art. 2º define al servicio de telecomunicación como aquél "cuya prestación consiste total o parcialmente en la transmisión y el envío de señales a través de redes de telecomunicación, excepción hecha de la radiodifusión sonora y de la televisión", y define a la red pública de telecomunicación como "los sistemas de transmisión y, cuando proceda, los equipos de conmutación y otros recursos que permiten la transmisión de señales entre puntos de terminación definidos por cable, por medios radioeléctricos, por medios ópticos o por otros medios electromagnéticos que se utilizan, total o parcialmente, para la prestación de servicios públicos de telecomunicación".

Agrega el art. 5º que "Los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente" (para proteger la seguridad nacional, la defensa, la seguridad pública, o para la detección y persecución de delitos).

En materia de tráfico y facturación, dispone el art. 6º que "los datos sobre tráfico relacionados con los usuarios y abonados tratados para establecer comunicaciones y almacenados por el proveedor de una red o servicio público de telecomunicación deberán destruirse o hacerse anónimos en cuanto termine la comunicación" (inc. 1º). "A los efectos de la facturación de los usuarios y de los pagos de las interconexiones, podrán ser tratados los datos indicados en el anexo" (que son: el número o la estación del abonado, la dirección del abonado y el tipo de estación, el número total de unidades que deben facturarse durante el ejercicio contable, el número del abonado que recibe la llamada, el tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos trasmitidos, la fecha de la llamada o del servicio, y otros datos relativos a los pagos), cuyo tratamiento se realizará "únicamente hasta la expiración del plazo durante el cual pueda

39. Ver: Carlos E. DELPIAZZO - «Derecho Informático Uruguayo» (Idea, Montevideo, 1995), pág. 215 y sigtes.
40. Ver: Manuel HEREDERO HIGUERAS - «La Directiva comunitaria de Protección de los Datos Personales» (Aranzadi, Pamplona, 1997).
41. Ver: Miguel Angel DAVARA RODRIGUEZ - "La protección de datos personales en el sector de las telecomunicaciones" (Madrid, 2000), pág. 71 y sigtes.

impugnarse legalmente la factura o exigirse el pago" (inc. 2º).

Cuando se ofrezca la posibilidad de presentar la identificación de la línea llamante, tanto el usuario que origine la llamada como el que la reciba deberá tener la posibilidad, mediante un procedimiento sencillo y gratuito, de suprimir la identificación de la línea llamante (art. 8º).

Según el art. 11, "Los datos personales recogidos en las guías impresas o electrónicas accesibles al público o que pueden obtenerse a través de servicios de información deberán limitarse a lo estrictamente necesario para identificar a un abonado concreto, a menos que el abonado haya dado su consentimiento inequívoco para que se publiquen otros datos personales. El abonado tendrá derecho, de forma gratuita, a que se le excluya de una guía impresa o electrónica a petición propia, a indicar que sus datos personales no se utilicen para fines de venta directa, a que se omita parcialmente su dirección y a que no exista referencia que revele su sexo, cuando ello sea aplicable lingüísticamente".

Finalmente, las llamadas con fines de venta directa son objeto de regulación en el art. 12, a cuyo tenor "sólo se podrán autorizar respecto de aquellos abonados que hayan dado su consentimiento previo".

En cuarto lugar, corresponde hacer mención a la Directiva del Parlamento Europeo y del Consejo Nº 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, la cual tuvo por objeto sustituir a la anterior Directiva Nº 97/66/CE con el propósito de adaptar sus soluciones al desarrollo de los mercados y de las tecnologías de los servicios de comunicaciones electrónicas disponibles al público, contemplando las redes móviles digitales e Internet y extendiendo las soluciones a las personas jurídicas.

En virtud de esta Directiva, se mantiene la obligación de preservar la seguridad a cargo de todo proveedor de un servicio de comunicaciones (art. 4º), entendiendo por tales "cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponibles para el público" (art. 2º, lit. d).

Se reitera igualmente la obligación de los Estados miembros de garantizar "la confidencialidad de las comunicaciones y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público" (art. 5º).

Asimismo, se mantiene la solución de que "los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponibles al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de transmisión de una comunicación" (art. 6º), sin perjuicio de los tratamientos necesarios para la facturación de los abonados y los pagos de interconexiones y de los que sean útiles para promoción comercial o prestación de servicios de valor añadido, en ambos casos con el consentimiento previo del abonado o usuario.

No obstante, se agrega que "En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico,… sólo podrán tratarse estos datos si se hacen anónimos o previo consentimiento de los usuarios o abonados" (art. 9º).

En cuanto a las guías de abonados, el art. 12 prevé que "Los Estados miembros velarán por que se informe gratuitamente a los abonados antes de ser incluidos en las guías acerca de los fines de las guías de abonados, impresas o electrónicas, disponibles al público o accesibles a través de servicios de información sobre las mismas, en las que puedan incluirse sus datos personales, así como de cualquier otra posibilidad de uso basada en funciones de búsqueda incorporadas en las versiones electrónicas de la guía". Añade que "La no inclusión en una guía pública de abonados, así como la comprobación, corrección o supresión de datos personales de una guía, no deberán dar lugar al cobro de cantidad alguna".

En materia de comunicaciones no solicitadas, dispone el art. 13 que "Sólo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo".

Obsérvese que en los instrumentos jurídicos reseñados los conceptos de seguridad y confidencialidad, así como el consentimiento del usuario resultan claves.

Con respecto a la *seguridad*, se ha entendido que la misma debe ser analizada y comprendida tanto como seguridad física, como seguridad lógica y como seguridad jurídica [42].

En materia de *confidencialidad*, lo que subyace es la expectativa que tienen los comunicantes a distancia de que lo comunicado es secreto, con independencia de que el contenido de la comunicación pueda o no ser

42. Miguel Angel DAVARA RODRIGUEZ - "Manual de Derecho Informático" (Aranzadi, Pamplona, 1997), pág. 33; y "La protección de datos personales en el sector de las telecomunicaciones" cit., 25 y sigtes.

calificado de íntimo [43]. Entiende la doctrina que el llamado derecho al secreto de las comunicaciones no abarca sólo su contenido sino también todas las circunstancias que las rodean, como la identidad de los interlocutores o el momento en el que se realizan [44].

Por lo que refiere al *consentimiento del interesado* para el tratamiento de sus datos, es un principio cardinal en la materia, el cual no puede disociarse de los principios de finalidad y licitud de la colecta [45].

En quinto lugar, cabe hacer referencia a la reciente aprobación de la Directiva del Parlamento Europeo y del Consejo sobre retención de datos telefónicos y de comunicaciones electrónicas, conforme a la cual se obliga a los proveedores a retener los datos de llamadas y de correo electrónico (con excepción de su contenido, sólo accesible por mandato judicial) por entre 6 y 24 meses.

Se trata de una normativa limitativa de la establecida precedentemente, con el objeto de luchar contra el terrorismo y el crimen organizado.

Paralelamente a la regulación multinacional, en muchos países, frente a los cambios experimentados en el campo de las telecomunicaciones, se ha visto la necesidad de dictar normas de **Derecho interno** destinadas a tutelar la privacidad como un aspecto conexo a la nueva regulación de las telecomunicaciones [46] o se ha encarado la aplicación directa de las leyes sobre protección de datos personales a los servicios de telecomunicaciones [47].

Así, el art. 50 de la *Ley General de Telecomunicaciones de España* Nº 11/1998 de 24 de abril de 1998 previó que "Los operadores que presten servicios de telecomunicaciones al público o exploten redes de telecomunicaciones accesibles al público deberán garantizar, en el ejercicio de su actividad, la protección de datos de carácter personal, conforme a lo dispuesto en la Ley Orgánica Nº 5/1992 de 29 de octubre, de regulación del Tratamiento Automatizado de los Datos de carácter Personal [48], en las normas dictadas en su desarrollo y en las normas reglamentarias de carácter técnico, cuya aprobación exija la normativa comunitaria en materia de protección de datos personales" [49].

Por su parte, la *Ley Orgánica de Telecomunicaciones de Venezuela* del año 2000 incluye en su art. 12, num. 2º, entre los derechos de todo usuario de servicios de telecomunicaciones, "la privacidad e inviolabilidad de sus telecomunicaciones salvo en aquellos casos expresamente autorizados por la Constitución o que, por su naturaleza, tengan carácter público" [50].

C) Situación uruguaya

En el Derecho nacional no existe normativa especial en materia de seguridad de los datos personales en el ámbito de los servicios de telecomunicaciones y la reciente ley Nº 17.838 de 24 de setiembre de 2004 refiere específicamente a la protección de los datos personales de carácter comercial, razón por lo cual la aplicación de sus normas a las telecomunicaciones no resulta sencilla, sin perjuicio de lo cual cabe rescatar la generalidad del alcance dado a la acción de habeas data y la explicitación de algunos principios generales en la materia cuya aplicación a las nuevas situaciones puede servir para resolverlas [51].

No obstante la ausencia de legislación específica, cabe hacer caudal de lo previsto en los arts. 7º, 10 y 72 de la Constitución para la tutela de la seguridad de los datos personales [52] y, especialmente, de lo que establece el art. 28 de la Constitución, cuya potencialidad aplicativa en la materia debe destacarse.

43. Miquel ROCA JUNYENT y Elisa TORRALBA MENDIOLA - "Derecho a la intimidad: el secreto de las comunicaciones e Internet", en A.A.V.V. - "Régimen jurídico de Internet" (La Ley Actualidad, Madrid, 2002), pág. 185.
44. R. MARTIN MORALES - "El régimen constitucional del secreto de las comunicaciones" (Civitas, Madrid, 1995), pág. 56.
45. Carlos E. DELPIAZZO - «Protección de los datos personales en tiempos de Internet. El nuevo rostro del derecho a la intimidad» cit., pág. 272; y "Historia clínica electrónica. A propósito de marco regulatorio en Uruguay", en X Congreso Iberoamericano de Derecho e Informática (Santiago de Chile, 2004), pág. 241 y sigtes.
46. José Luis MONTOTO GUERRIERO - "Aspectos conexos a la regulación de las telecomunicaciones. Privacidad", en Rev. La Ley, Año LXIV, Nº 234, págs. 1 y 2.
47. Agustín DE ASIS ROIG - "Protección de datos y Derecho de las telecomunicaciones" cit., pág. 204 y sigtes.
48. La Ley Orgánica Nº 5/1992 de 29 de octubre de 1992 (LORTAD) fue sustituida por la Ley Orgánica Nº 15/1999 de 13 de diciembre de 1999 de Protección de Datos de carácter Personal (LOPD). Ver su texto en: anuario "Derecho Informático" (F.C.U., Montevideo, 2001), tomo I, pág. 379 y sigtes.
49. Ver: L. MARTIN RETORTILLO - "Artículo 50", en Eduardo GARCIA DE ENTERRIA y Tomás QUADRA SALCEDO - "Comentarios a la Ley General de Telecomunicaciones (Ley Nº 11/1998 de 24 de abril)" (Civitas, Madrid, 1999).
50. Ver: Rafael BADELL MADRID y José Ignacio HERNANDEZ - "Régimen Jurídico de las Telecomunicaciones en Venezuela" (Caracas, 2002), pág. 131.
51. Carlos E. DELPIAZZO - "Primera lectura de la ley Nº 17.838 de 24 de setiembre de 2004", en anuario "Derecho Informático" (F.C.U., Montevideo, 2005), tomo V.
52. Carlos E. DELPIAZZO - "Estado de la protección de datos personales en Uruguay", en anuario "Derecho Informático" (F.C.U., Montevideo, 2004), tomo IV, pág. 271 y sigtes.; "Posibles medios de protección frente a las responsabilidades derivadas de la gestión de bases

Al tenor de dicha norma que, con leves variantes de redacción, proviene de nuestra primera Constitución patria de 1830 (art. 140), "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general".

La referencia a la correspondencia "telegráfica o de cualquier otra naturaleza", agregada en la reforma constitucional de 1934 (art. 27), merece ser destacada por cuanto, "dirigida a evitar cualquier absurda interpretación excluyente, asegura la inclusión de las comunicaciones telefónicas en el concepto de correspondencia. Pero además, impone ahora, la aplicación del texto a cualquier medio o instrumento de comunicación que el progreso científico o tecnológico pueda generar en el futuro" (53), de modo que "asegura al texto constitucional una actualidad plurisecular, en la medida que torna posible la adecuación constante de los principios allí contenidos a los nuevos avances técnicos" (54).

Según calificada opinión, "Es fundamental destacar que la norma constitucional garantiza no sólo la inviolabilidad del contenido de las conversaciones telefónicas sino también -como consecuencia de la prohibición de su registro- la inviolabilidad de toda lista o nómina de las llamadas que se han hecho, de qué llamadas se han recibido, y de entre quiénes y cuándo... La inviolabilidad cubre no sólo el contenido sino la existencia misma de las comunicaciones telefónicas y, por ende, su difusión y conocimiento por terceros» (55).

Nótese que los tres vocablos nucleares que definen las conductas prohibidas incluidas en la disposición son "registro, examen o interceptación", los cuales, especialmente los dos primeros, encartan a mi juicio el tratamiento de los datos personales con el sentido que a la expresión tratamiento le atribuye el art. 1º, inc. 2º de la ley Nº 17.838 como "toda forma de registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración y toda otra forma del mismo o similar alcance" (56).

En primer término, "*Registrar* es no sólo examinar el contenido de algo, sino también anotar, inscribir o enumerar, según resulta del Diccionario de la Real Academia Española. Entre dos acepciones de la palabra registrar, una que implica examinar, lo que significa considerar el contenido, y otra que se refiere a anotar, ambas enumeradas en el Diccionario de la Real Academia Española, el intérprete, para dar sentido al art. 28, debe optar por la acepción compatible con la más amplia protección de la libertad y la mayor limitación del poder público. Es, en el caso, la aplicación del principio hermenéutico pro hominis y la que tiene en cuenta, teleológicamente, el fin y el objeto de la norma constitucional. Y esto es además, lógico, porque comunicar una lista de llamadas hechas o recibidas, constituye -y con efectos eventualmente graves- un serio atentado a la inviolabilidad de la correspondencia telefónica" (57).

En segundo término, "*examinar*" quiere decir investigar, indagar, estudiar o analizar, en el caso, fundamentalmente el contenido de las comunicaciones de que se trate.

En tercer lugar, si bien en su sentido natural "*interceptar*" quiere decir detener el pasaje de algo o impedir que llegue al lugar al que se dirige, con referencia a las telecomunicaciones en general y a las comunicaciones telefónicas en particular, implica la ingerencia externa, un acto de un tercero, ajeno a los interlocutores, y que actúa sin consentimiento por lo menos de uno de ellos, a los efectos de tomar conocimiento del contenido de una conversación que de otro modo le sería desconocida, ya sea que se registre o no la misma en una cinta magnetofónica (58).

Sólo la ley formal, por razones de interés general, puede privar (en el sentido del art. 7º de la Constitución) de la protección constitucional del art. 28, de modo que la interceptación telefónica, aún con fines probatorios, para que sea legítima, requiere estar soportada en una norma habilitante de rango legal (59).

de datos en el Derecho uruguayo", en Congreso Internacional de Informática y Derecho (Buenos Aires, 1990), pág. 382 y sigtes.; y «Tratamiento jurídico de los datos personales en Uruguay», en CD del X Congreso iberoamericano de Derecho e Informática (Santiago de Chile, 2004).

53. Héctor GROS ESPIELL - "El artículo 28 de la Constitución y las comunicaciones telefónicas", en Rev. de Administración Pública Uruguaya, Nº 25, pág. 84.
54. Bernadette MINVIELLE - "El derecho a la intimidad y la prueba en el proceso penal, con especial referencia a las interceptaciones telefónicas", en Rev. Uruguaya de Derecho Procesal, Año 1985, Nº 2, pág. 154.
55. Héctor GROS ESPIELL - "El artículo 28 de la Constitución y las comunicaciones telefónicas" cit., pág. 86.
56. Carlos E. DELPIAZZO - «Primera lectura de la ley Nº 17.838 de 24 de setiembre de 2004», en anuario "Derecho Informático" (F.C.U., Montevideo, 2005), tomo V, pág. 451 y sigtes.; "Acerca de la ley Nº 17.838", en Rev. de la Liga de Defensa Comercial (Montevideo, 2004), Nº 138, pág. 14 y sigtes.; "Las nuevas tecnologías en el Uruguay. Impacto de Internet sobre la persona", en XV aniversario del Anuario de Derecho Administrativo (F.C.U., Montevideo, 2005), pág. 39 y sigtes.; y "El derecho a la intimidad en el nuevo horizonte telecomunicativo", en CD del XI Congreso Iberoamericano de Derecho e Informática" (Panamá, 2006).
57. Héctor GROS ESPIELL - "El artículo 28 de la Constitución y las comunicaciones telefónicas" cit., págs. 86 y 87.
58. Bernadette MINVIELLE - "El derecho a la intimidad y la prueba en el proceso penal, con especial referencia a las interceptaciones telefónicas" cit., págs. 158 y 159.
59. Bernadette MINVIELLE - "El derecho a la intimidad y la prueba en el proceso penal, con especial referencia a las interceptaciones telefónicas" cit., pág. 167 y sigtes.