LA PROTECCION DE DATOS PERSONALES EN LAS EMPRESAS DE TELECOMUNICACIONES EN EL PERÚ

Elizabeth Cornejo Espilco[1]

SUMILLA: 1. Introducción. 2. La protección de datos en las empresas de telecomunicaciones del Perú; 2.1. Aspectos generales; 2.2 Ámbito de protección y vulneraciones; 2.3. Las obligaciones de las empresas operadoras de telecomunicaciones; 2.4. Pautas generales de seguridad; 2.5 Implementación de medidas y procedimientos; 2.6. Informes de los operadores de telecomunicaciones; 2.7. Control por parte del Ministerio de Transportes y Comunicaciones; 2.8. Responsabilidades por incumplimiento de obligaciones. 3. Conclusiones. 4. Bibliografía.

1. INTRODUCCIÓN.

La incidencia de los datos personales en el Derecho, a lo largo de la historia, es de antigua data, aunque su reconocimiento como derecho subjetivo a nivel constitucional y por la jurisprudencia es reciente en los últimos cuarenta años, motivando que se le regule tanto en el plano internacional como en el ordenamiento interno de cada país.

[1] Abogada por la Universidad Particular de San Martín de Porres (Lima - Perú). Se desempeña como Asesora Legal de América Móvil Perú SAC (Claro Perú). Especialista en Derecho de las Telecomunicaciones. Tiene estudios de Postgrado en Derecho Minero y Derecho Ambiental en la Universidad Nacional Mayor de San Marcos (Lima – Perú). Ha intervenido como conferencista, panelista y ponente y efectuado publicaciones, en materia de Derecho de las Telecomunicaciones, Derecho Constitucional, Derecho Administrativo, Derecho Penal y Derecho Procesal Penal. Las opiniones vertidas en el presente trabajo, no comprometen a la empresa en la cual laboro.

Sin embargo, en los últimos veinte años, la importancia del tratamiento jurídico de los datos personales se ha venido incrementando de manera exorbitante, debido al avance de las tecnologías de la información y de las telecomunicaciones[2], que han originado el desarrollo de bases de datos de las personas, tanto en los organismos estatales como en empresas privadas.

Tal como manifiesta Marcelo Bauzá Reilly[3], se trata de un derecho fundamental que se encuentra evolucionando de manera permanente y viene siendo reconocido normativamente en los países latinoamericanos, a través de la confluencia de modelos jurídicos reconocibles y vigentes.

Tanto en la doctrina como en la jurisprudencia del Perú y del Derecho Comparado, se han vertido varias denominaciones vinculadas a los datos personales como derecho subjetivo, tales como "derecho a la autodeterminación informativa", aunque nos parece correcto utilizar la frase propuesta por Leysser León[4]: ***Los derechos sobre los datos personales***; para describir el desarrollo doctrinal y legislativo actual en esta materia.

Se considera que este derecho constitucional supone la facultad que tienen las personas para controlar y disponer sobre el acopio y uso de los datos referidos a ellos, almacenados en registros o bancos de datos públicos o privados, sin que se refiera necesariamente dicha información a aspectos íntimos[5].

Este concepto responde al carácter formal que tiene este derecho, al servir de sustento para la protección de otros derechos, como la intimidad, la vida privada, la identidad, el honor y la propia imagen; así como reconoce su autonomía frente a

---

[2] ZAMUDIO Salinas, María de Lourdes. *Situación de la protección normativa de los datos personales en el Perú*.

[3] *El actual derecho de la protección de datos en América y Europa*. En: "Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección de la persona y derechos fundamentales". 2006, pág. 41.

[4] LEYSSER L. León, Hilario. *El Problema Jurídico de la Manipulación de Información Personal*. Palestra Editores, Lima, 2007.

[5] CASTRO Cruzatt, Karin. *El derecho fundamental a la protección de datos personales o autodeterminación informativa*. En: Los derechos fundamentales. Estudios de los derechos constitucionales desde las diversas especialidades del Derecho. Lima, Gaceta Jurídica Editores, 2010, págs. 171-172.

estos mismos derechos, especialmente con la intimidad y la vida privada, con los que se relacionó a la protección de los datos personales en sus inicios.

Este derecho ha sido incorporado al ordenamiento jurídico peruano, mediante el artículo 2° inciso 6 de la Constitución Política de 1993[6], aunque influenciado por el desarrollo doctrinal de la época se le vinculaba con el derecho a la intimidad, posteriormente diversos estudios y jurisprudencia han establecido relaciones con otros derechos constitucionales como son la identidad, el honor y la propia imagen. Por otro lado, se regula la protección constitucional del derecho materia de estudio, que se da a través de la acción de habeas data regulado en el inciso 3 del artículo 200 de la acotada Constitución[7],

Esta correlación se plasma en el artículo 1° del Proyecto de la Ley de Protección de Datos Personales, publicado el 23 de julio del año 2004, y que lamentablemente, hasta el momento, no ha sido promulgado como Ley, impidiendo que exista una norma de desarrollo constitucional que permita una mejor protección de los datos personales de las personas[8].

En este proyecto, se hace una importante distinción entre dato personal y dato sensible, considerando al primero como la información concerniente a personas naturales, identificadas o identificables, mientras que el segundo viene a ser todo

---

[6] *"Artículo 2°.- Derechos fundamentales de la persona.*
Toda persona tiene derecho:
(…)
6.- A que los servicios informáticos, computarizados o no, públicos o privados no suministren informaciones que afecten la intimidad personal y familiar."

[7] "*Artículo 200.- Acciones de garantía constitucional.*
Son garantía constitucionales:
(…)
3. La Acción de Habeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2°, incisos 5 y 6 de la Constitución."

[8] Esperamos que el reciente acuerdo realizado entre los países latinoamericanos y la Comunidad Europea, en este mes de mayo de 2010, sirva de impulso en el Perú, para que se promulgue tan ansiada Ley de Protección de Datos Personales, tomando como base lo expresado por la Directora de Área de Derechos Ciudadanos de AGESIC, D. Viega, en cuanto a que algunas de las ventajas de la promulgación de la Ley 18.331 en Uruguay, que regula la protección de datos en ese país, han sido la búsqueda de reconocimiento de la Unión Europea como un país seguro para el envío de datos personales y la captación de inversores. Cita efectuada por SARASOLA, Florencia. *Ley de protección de datos personales*. Facultad de Ingeniería de la Universidad ORT de Uruguay, 2009, pág. 7.

dato de una persona natural relacionado al origen racial y étnica, opinión política, convicción religiosa filosófica o moral, afiliación sindical a la salud o a la vida sexual, entre otros legalmente establecidos en esa calidad.

No obstante, se encuentran diversas normas en el espectro jurídico peruano, que regulan algunos casos especiales de manejo de bases de datos en entidades privadas, tal como la Ley N° 27849, que regula el suministro que efectúan las centrales privadas de información de riesgos, que comprende a los datos relacionados a las obligaciones o antecedentes financieros, comerciales, tributarios, laborales y de seguros, de una persona natural o jurídica que permita evaluar sus solvencia económica; así como, se reglamenta lo relativo a la protección del titular de esa información de riesgos, excluyéndose de la misma a la información sensible[9].

Otra norma relacionada pero referente al tratamiento de bases de datos personales en el sector público, es la Ley de Transparencia y Acceso a la Información Pública y su Reglamento[10], donde se establece en el inciso 5 del artículo 17°, a los datos personales como información que no puede ser difundida mediante la aplicación de esa norma, salvo autorización judicial.

A continuación, se esbozará principalmente, sobre cómo se regula la protección de los datos personales de los usuarios y/o abonados de los servicios que prestan las empresas de telecomunicaciones peruanas, que en su gran mayoría, pertenecen al ámbito privado, otorgando de esta manera, una singularidad sobre el manejo de las bases de datos por parte de estas empresas, donde su tratamiento se conjuga con los datos relacionados a otro derecho fundamental como es el secreto de las comunicaciones y que a veces suele ocasionar problemas prácticos en su distinción, por parte de algunos operadores jurídicos, lo que también se refleja en la legislación administrativa peruana, como se analizará más adelante.

[9] Según el artículo 2° de dicha Ley, se considera a todo dato referido a las características físicas, morales o emocionales de una persona natural, o a hechos o circunstancias de su vida afectiva o familiar, tales como los hábitos personales, las ideologías, y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual u otras análogas que afecten su intimidad y todo lo referido en la Constitución Política del Perú en su artículo 2° inciso 6.

[10] Mediante el Decreto Supremo N° 043-2003-PCM, publicado en el Diario Oficial El Peruano, el 24 de abril de 2003, se aprueba su Texto Único Ordenado; mientras que su Reglamento se aprobó por Decreto Supremo N° 072-2003-PCM, publicado el 7 de agosto de ese mismo año, en el Diario Oficial El Peruano.

2. LA PROTECCIÓN DE DATOS EN LAS EMPRESAS DE TELECOMUNICACIONES DEL PERÚ.

2.1 Aspectos Generales.

Siguiendo los lineamientos constitucionales, el artículo 4° del Texto Único Ordenado de la Ley de Telecomunicaciones, aprobado por Decreto Supremo N° 013-93-TCC[11], señala que toda persona tiene derecho al secreto de las comunicaciones y encarga al Ministerio de Transportes y Comunicaciones (en adelante, el MTC) proteger ese derecho. Posteriormente, mediante el artículo 13° del Reglamento de la Ley de Telecomunicaciones, cuyo Texto Único Ordenado fue aprobado por Decreto Supremo Nº 020-2007-MTC[12], se amplió la protección jurídica administrativa a los datos personales, estableciendo que los concesionarios de los servicios públicos de telecomunicaciones deben mantener la confidencialidad de la información personal relativa a sus usuarios que se hubieran obtenido en el curso de sus negocios, salvo consentimiento previo, expreso y por escrito de sus usuarios y demás partes involucradas o por mandato judicial.

Como se puede apreciar, en estas dos normas acotadas, se expresa la evolución en el reconocimiento en el Perú sobre el derecho sobre los datos personales, incluso, la actual redacción del aludido artículo 13° del Reglamento, recoge varios puntos propuestos en el nombrado Proyecto de Ley de Protección de Datos Personales.

Dentro de las medidas que la dimensión objetiva del derecho sobre los datos personales, obliga a dictar al Estado Peruano, para proteger este derecho, es que con fecha 07 de febrero del 2009, se publicó en el Diario Oficial El Peruano, la Resolución Ministerial Nº 111-2009-MTC/03 (en adelante, la Resolución Ministerial), que aprueba la norma que establece las medidas destinadas a salvaguardar el Derecho a la Inviolabilidad y el Secreto de las Telecomunicaciones y la Protección de Datos

[11] Publicado el 6 de mayo de 1993, en el Diario Oficial El Peruano.

[12] Publicado el 4 de julio de 2007, en el Diario Oficial El Peruano.

Personales; así como regular las acciones de supervisión y control a cargo del MTC[13]; derogándose la Resolución Ministerial Nº 622-96-MTC-16.17, que aprobó la Directiva Nº 002-96-MTC/15.17, que regulaba este tema y que se concentraba en regular la protección del derecho al secreto de las comunicaciones.

Conforme a lo que se expresa en el glosario de la Resolución Ministerial Nº 011-2009-MTC/03, se entiende como protección de datos personales a la obligación que tienen las empresas de telecomunicaciones para adoptar las medidas necesarias, a fin que la información personal obtenida de sus abonados[14] o usuarios[15], en el curso de sus operaciones comerciales, no sea obtenido por terceros, salvo las excepciones señaladas en dicha norma y que estudiaremos más adelante. Este concepto está restringido en su aplicación por el ámbito de las telecomunicaciones y desde el ángulo de las empresas operadoras, sin desarrollar los derechos de los usuarios o abonados, que deberán ser protegidos por estas empresas, aunque reconocemos que esto último se enmarca más dentro del ámbito del derecho del consumidor[16]. Por otro lado, esta definición reconoce el fenómeno del desplazamiento del poder de control de la información personal hacia un tercero que pertenece al sector privado y que adquiere datos de los individuos, como consecuencia de las operaciones comerciales que realizan con sus consumidores.

---

[13] Debemos mencionar que el día 23 de enero del presente año, el MTC publicó en el Diario Oficial El Peruano, el proyecto de Resolución Ministerial objeto de este estudio.

[14] Para efectos del presente trabajo, se entiende por abonado al usuario que celebra un contrato de prestación de servicios de telecomunicaciones con una empresa explotadora de servicios públicos; mientras que, usuario es todo aquel que utilice los servicios de telecomunicaciones.

[15] Es la persona natural o jurídica que en forma eventual o permanente tiene acceso a algún servicio público o privado de telecomunicaciones. Es quien utiliza el servicio, sin ostentar necesariamente la calidad de titular. Por ejemplo, Scarlett adquiere un Pack Pre Pago (equipo y línea) y permite a Frank su uso; este último viene a ser el usuario, mientras que Scarlett tendría la calidad de abonada.

[16] Siguiendo a ESPINOZA Espinoza, Juan. *Derecho de las Personas*. Cuarta edición. Lima, Gaceta Jurídica, 2004, pág. 413, entre los derechos que tendrían los usuarios y abonados, encontramos:

a) Acceder a la información.
b) Solicitar la rectificación o cancelación de datos inexactos o caducos.
c) Exigir que los datos sean utilizados de acuerdo al fin por el cual se recogieron.
d) Insertar información personal como si es presupuesto por obtener alguna prestación.
e) A que no se emita un juicio de valor judicial, administrativo o privado que se sustente en un tratamiento informatizado de datos que permitan establecer un perfil o delaten la personalidad del interesado o del consumidor.

Concordamos más bien con Juan Rivadeneyra Sánchez[17], quien manifiesta que los datos personales no guardan relación alguna ni con la existencia ni con el contenido de la comunicación, más bien se trata de información relevante que una persona brinda al momento de contratar la provisión de un servicio de telecomunicaciones.

Del análisis de la nombrada Resolución, se aprecia una mejora en cuanto al enfoque de la finalidad, en comparación a la norma derogada[18], puesto que lo primordial en este nivel de regulación, es la obligación que tienen los operadores para proteger el secreto de las comunicaciones y los datos personales de sus usuario y/o abonados; para lo cual, el MTC se encargará de velar el cumplimiento de esa obligación.

Respecto al ámbito de aplicación de la norma, debemos señalar que a diferencia de lo estipulado en la Directiva derogada, que se dirigía a todas las empresas operadoras de telecomunicaciones; actualmente, los alcances abarcan tanto a personas naturales como jurídicas que presten estos servicios y se hacen dos precisiones:

- En el caso que un operador de servicios públicos de telecomunicaciones financiado por FITEL[19], hace uso de los servicios de transmisión de voz y/o datos de un operador de servicio privado, la responsabilidad recaerá en el primer operador.

- Se reduce la aplicación a la protección de datos y no al secreto de las telecomunicaciones, cuando los operadores sólo presten servicio público de distribución de radiodifusión por cable[20] y no brinden servicios de valor añadido que se sustenten en la red de cable o servicios convergentes de telefonía fija y/o acceso a Internet.

---

[17] *Algunas Consideraciones Básicas sobre la Protección del Secreto e inviolabilidad de las comunicaciones telefónicas.* En Advocatus N° 14, Año 2006-I, Lima, pág. 338.

[18] La finalidad giraba en torno a las facultades inspectivas del MTC.

[19] Fondo de Inversión de las Telecomunicaciones, creado por el artículo 12º de la Ley de Telecomunicaciones y que se encuentra a cargo de OSIPTEL, tiene como meta, buscar el acceso para todas las personas, especialmente en áreas rurales y de interés social, a los distintos servicios públicos de telecomunicaciones, es lo que se conoce como “el acceso universal”.

[20] Llamado también televisión cerrada o por cable.

2.2 Ámbito de Protección y Vulneraciones.

Posteriormente, la referida Resolución Ministerial describe el ámbito de protección del derecho al secreto de las comunicaciones y del derecho a los datos personales, debemos señalar que la norma en mención, no distingue el ámbito de protección entre ambos derechos, lo cual ocasiona confusión en la práctica, tanto para las empresas operadoras como para los usuarios y órganos jurisdiccionales, respecto a cuándo proceden las solicitudes por el levantamiento del secreto de las comunicaciones y cuándo las peticiones se refieren a datos personales; no obstante, con el concepto vertido sobre protección de datos personales, se puede establecer los siguientes aspectos que corresponde al ámbito de protección del derecho fundamental materia de estudio:

a) *La información personal que los operadores de telecomunicaciones obtengan de sus abonados o usuarios en el curso de sus operaciones comerciales* y que estén contenidas en soporte físico, informático o similares, en tanto dicho usuario o abonado no haya autorizado su difusión o esté permitida por el marco legal vigente. Entre esa información personal, se debe considerar a las denominadas "generales de ley" del titular de la línea o usuario (dirección domiciliaria, Documento Nacional de Identidad, estado civil, ocupación o profesión, teléfono de referencia, modalidad y comportamiento de pago).

b) *Histórico de pedidos* (traslados, cambio de número, avería, boletines de reparación, hojas de visita, cambio de plan, etc.).

Consideramos que también sobre esta materia hay omisiones en la aludida Resolución Ministerial N° 111-2009-MTC/03 y que debieron haberse incluido a fin de proteger con mayor eficacia, los derechos a los datos personales de los usuarios y/o abonados. Entre estas omisiones tenemos:

a) *Información sobre datos personales del usuario y/o titular que envió mensajes de texto desde la página Web de la Empresa de Telecomunicaciones*. Este es el caso, cuando un usuario desea enviar un mensaje de texto desde la página Web de la empresa de Telecomunicaciones, se le solicita sus datos personales (nombre, dirección domiciliaria, DNI, etc.) por cuestiones de seguridad, esta

información queda almacenada en la base de datos de las diversas empresas que prestan estos servicios, la cantidad de información requerida depende de cada operador.

b) *Información sobre si o no es cliente de la empresa operadora*.

c) *Modalidad de servicio (Post Pago y Pre Pago)*.

En cambio, se produce una afectación cuando la información relativa a abonados o usuarios es entregada a terceros no autorizados, sin las garantías de ley[21], especialmente las vinculadas a la intimidad personal y/o familiar de aquellos. Entre las excepciones que contempla la mencionada Resolución Ministerial, que no constituyen afectación al derecho que se alude, tenemos[22]:

a) La entrega de información a terceros que participen en la gestión comercial de servicios del operador de telecomunicaciones, siempre que esos datos sean necesarios para el cumplimiento de ese fin mercantil.

b) La entrega de información a las centrales de riesgo, al Poder Judicial, al Organismo Supervisor de la Inversión Privada en Telecomunicaciones - OSIPTEL, al Administrador de la Base de Datos de Portabilidad Numérica, otros Operadores de Telecomunicaciones y a otras entidades habilitadas, según la legislación vigente.

c) Lo que se publica en las guías de abonados[23].

Para una adecuada protección, la citada Resolución Ministerial establece la obligación a los operadores, para que instalen medidas de seguridad concernientes a proteger la información contenida en los recibos de servicios telefónicos, requerimientos de pago y otros comprobantes de pago (boletas, facturas, notas de

---

[21] Que no medie resolución judicial o autorización expresa del abonado o usuario.

[22] Concordamos con RIVADENEYRA, op. cit., pág. 339, en que la autorización que realiza el propio titular del derecho no es una excepción sino que se trata de un acto voluntario.

[23] Debemos señalar que en la Comunidad Europea, mediante la Directiva N° 2002/58/CE del 12 de julio de 2002, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el sector de las comunicaciones electrónicas, se establece que sus estados miembros deben velar para que sus abonados tengan la oportunidad de decidir si sus datos personales figurarán o no en una guía pública, y, de ser el caso, indicar qué datos se publicarán. Ésta es una medida que debió incluirse en la norma que se comenta.

crédito y débito), así como la información referida a detalles de llamadas (no incluidas en recibos), historial de suspensiones, cortes y reconexiones y grabaciones por gestiones de deuda.

2.3 Obligaciones de los Operadores de Telecomunicaciones.

Sustentándose en lo dispuesto en el artículo 13° del Reglamento de la Ley de Telecomunicaciones, la Resolución Ministerial que se comenta, establece las siguientes obligaciones a los operadores:

1) Respetar y salvaguardar el secreto de las telecomunicaciones y proteger los datos personales de sus abonados y/o usuarios, salvo las excepciones previstas en el ordenamiento jurídico, que son:

   - Consentimiento previo, expreso y por escrito del abonado y demás partes involucradas.
   - Mandato judicial debidamente motivado.

   Consideramos que no debe incluirse como excepción, a la información que el MTC podría requerir a los Operadores, en el caso de las llamadas maliciosas, que se regula en la Resolución Ministerial Nº 042-88-TC/TEL del 20 de julio de 1988, por cuanto la misma contradice abiertamente al Reglamento de la Ley de Telecomunicaciones, lo que se requiere, es una nueva regulación.

2) Brindar a la Dirección General de Control del MTC, todas las facilidades necesarias para que éstas cumplan sus funciones de inspección y verificación, sin necesidad de realizar previa notificación del ejercicio de esas funciones[24].

3) Implementar las medidas y procedimientos que resulten razonables, siguiendo los lineamientos de la Resolución Ministerial, así como todos aquellos complementarios que sirvan para cumplir con la primera de las obligaciones

[24] Esta obligación se sustenta en lo previsto en el artículo 116° de la Ley de Telecomunicaciones, que además obliga a los Operadores a mantener los registros detallados de sus operaciones comerciales con sus usuarios por los servicios que presta, lo cual debe ser puesto a disposición del MTC y OSIPTEL, con previo requerimiento, salvaguardando el derecho al secreto de las telecomunicaciones.

descritas; tomando en consideración, las redes y tecnologías que los Operadores empleen, conjuntamente al personal propio o de terceros que tenga acceso a la red pública o a la información confidencial de sus abonados y/o usuarios.

4) Las empresas operadoras tienen la obligación de presentar a la Dirección General de Control del MTC, un informe anual sobre las medidas y procedimientos adoptados para cumplir con la obligación mencionada en el numeral primero que antecede, debiendo presentarse la información a más tardar el 15 de febrero de cada año.

2.4 Pautas Generales de seguridad.

A fin que las empresas operadoras cumplan eficazmente con las obligaciones señaladas en el acápite anterior, la mencionada Resolución Ministerial recomienda seguir las pautas establecidas en tres documentos guías que se tratan sobre la adopción de medidas y procedimientos complementarios a los previstos en dicha norma, para la protección del derecho al secreto de las telecomunicaciones y de los datos personales de sus abonados y/o usuarios.

A continuación, realizaremos un breve resumen de estos importantes documentos, en los aspectos más vinculados a lo que se está desarrollando en el presente trabajo.

1) ***Norma Técnica Peruana N° NTP-ISO/IEC 1779 2007 EDI. Tecnología de la Información.***

Establece un código de buenas prácticas para la gestión de la seguridad de la información, fue aprobada por la Comisión de Reglamentos Técnicos y Comerciales del Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual – INDECOPI, mediante Resolución N° 001-2007-INDECOPI-CRT, de fecha 05 de enero de 2007.

Entre las principales guías, tenemos que estas prácticas tienen entre sus finalidades: la protección de datos de carácter personal y la intimidad de las personas, así como la salvaguarda de los datos de la organización (aquí se comprende a las clases de datos que registran los operadores) y los derechos de

propiedad intelectual, estableciendo guías de implementación para la protección de estos aspectos.

También desarrolla las medidas en materia laboral que se deben adoptar al interior de cada Operador de Telecomunicaciones, como funciones y responsabilidades del personal, la selección y política de personal, qué deben contener los acuerdos de confidencialidad, formación laboral, entre otras medidas. Igualmente, como en los documentos de la Unión Internacional de Telecomunicaciones, señalan las medidas, procedimientos y la gestión de la seguridad de la información a adoptarse por los Operadores.

2) ***Recomendación N° E.408 de la Unión Internacional de Telecomunicaciones***.

Referida a los "Requisitos de seguridad para las redes de telecomunicaciones". Entre sus principales sugerencias figura, que para establecer una eficiente seguridad en las redes de telecomunicaciones, se debe tomar en cuenta seis niveles: para el gestor de la red, seguridad física, supervisión, programas informáticos, herramientas de seguridad y auditoria de seguridad.

De esta manera, se podrá afrontar las amenazas que pudiesen afectar la seguridad en las redes, tanto a la confidencialidad como en la integridad de los datos y del sistema operativo. Otro aspecto relevante, es que estas medidas de seguridad deberán soportar la interceptación jurídica y el acceso a los datos de gestión por parte de los departamentos de justicia.

3) Manual sobre "La Seguridad de las Telecomunicaciones y las Tecnologías de la Información" de la Unión Internacional de Telecomunicaciones, edición 2006 y versiones actualizadas.

Entre los aportes más significativos tenemos lo referente a los fundamentos de la protección, diferenciando las amenazas entre accidentales[25] o intencionales[26], así

[25] Es aquella no premeditada, como puede ser un disfuncionamiento o fallo físico de un sistema o software.

[26] Es la que realiza una persona como un acto deliberado, aquí la amenaza se convierte en ataque a la seguridad.

como activas[27] o pasivas[28]. Asimismo, se realiza un desarrollo profundo de conceptos técnicos en materia de seguridad de la información, cuya aplicación se ve orientada con mayor arraigo en el área de ingeniería.

Siguiendo los lineamientos de los nombrados documentos emitidos por la Unión Internacional de Comunicaciones, en la Resolución Ministerial N° 111-2009-MTC/03, se incorporan los siguientes aspectos marco que sirven para establecer las medidas y procedimientos de seguridad que deben adoptar los operadores:

a) **Autenticación:** Significa corroborar que una entidad participante de la comunicación (persona, dispositivo, servicio y/o aplicación) tiene la identidad que dice ostentar, proporcionando confiabilidad a la comunicación; de este modo, se intenta evitar la usurpación de identidad o impedir la reproducción de una comunicación anterior sin autorización[29].

b) **Control de Acceso:** Implica que sólo el personal o los dispositivos autorizados puedan acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones, es decir, se protege el uso de recurso de red sin autorización. Debemos señalar que este marco está íntimamente vinculado al anterior por cuanto antes de conceder los accesos, debe verificarse la identidad de quien solicita los accesos.

c) **No Repudio:** Implica contar con la capacidad de evitar que una entidad (personal, dispositivos, servicios y/o aplicaciones), pueda negar haber realizado una acción en etapas posteriores. Supone además, la creación de pruebas que, en ocasiones posteriores, podrían ser utilizadas para demostrar

[27] Es la que se produce por un cambio de estado, por ejemplo alteración de datos o destrucción de equipos físicos.

[28] Aquí no se ocasiona ningún cambio de estado, el caso más emblemático es la denominada escucha clandestina.

[29] Un ejemplo que usualmente sucede es cuando se tiene que reportar el hurto, robo o pérdida de celular. En este caso, el usuario está en la obligación de reportar lo acontecido a la empresa que brinda el servicio de telecomunicaciones, quien solicitará los datos personales que el usuario brindó al momento de celebrar el contrato de prestación de servicios, tales como el número de DNI, con la finalidad de corroborar que la información dada es la que aparece en el registro privado de abonados de dicha operadora, y producida la confirmación, se procede a la suspensión del servicio y bloqueo del equipo lo que se reporta ante el Registro Nacional de Terminales de Telefonía Celular.

la falsedad de un argumento. La finalidad es determinar responsabilidades concretas sobre qué y quién ha hecho tal acción.

d) **Confidencialidad:** Implica que la información no se divulgará ni se pondrá a disposición de individuos, entidades o procesos no autorizados, para lo cual se podrán utilizar métodos como encriptación[30], listas de control de acceso y permisos de acceso.

e) **Integridad de los Datos:** Implica verificar que los datos personales no han sido alterados sin la autorización respectiva[31]. Respecto a este marco, debemos indicar que del análisis de los manuales emitidos por la Unión Internacional de Telecomunicaciones, sirvieron de sustento para la redacción de esta norma, se aprecia que no sólo debe abarcar lo concerniente a los datos personales, sino también a los datos de la comunicación, por cuanto éstos también se resguardan en base de datos a los cuales se tienen que aplicar pautas de seguridad; por lo que, sería recomendable realizar una modificación acerca de este punto.

f) **Alarma de Seguridad:** Mecanismo para detectar un evento relacionado con la seguridad, mediante la generación de un mensaje; se trata en realidad de una gestión de sistemas que describe el proceso de notificación que se origina por la recopilación de eventos de seguridad, las que finalmente serán objeto de auditoria para identificar los probables cambios de control, de políticas y procedimientos en la empresa operadora de telecomunicaciones.

Finalmente, la norma exige a los operadores que estén preparadas para afrontar la eventual demanda por el uso de un servicio especial, las comunicaciones que utilicen técnicas de cifrado de extremo a extremo. Mediante esta técnica, se transforma datos para que solamente sean entendibles a usuarios o personal

[30] Es la actividad que consiste en ocultar y descifrar información mediante técnicas especiales, se utiliza para el intercambio de mensajes, garantizando el secreto de la comunicación entre dos entidades y asegurar así que la información enviada sea auténtica, tanto respecto a que el remitente es quien dice ser y que el contenido del mensaje no ha sido modificado durante su trayectoria.

[31] Se han dado casos en algunas empresas operadoras, en el cual algunos usuarios han cambiado su situación jurídica debido a que fueron objeto de una adopción y, por tanto, cambian los apellidos – es aquí cuando éste solicita se actualice los datos en la base de datos de la operadora.

autorizado. Como se podrá apreciar, esto implica niveles de seguridad más desarrollados.

2.5 Implementación de medidas y procedimientos.

Los operadores deben realizar las siguientes acciones de implementación de medidas y procedimientos para salvaguardar el derecho al secreto de las telecomunicaciones y protección de datos[32]:

1) Garantizar a través de las medidas y procedimientos establecidos, que únicamente el personal debidamente autorizado, sea propio o de terceros, accedan a las instalaciones y sistemas con acceso restringido, previamente determinados por el operador de telecomunicaciones, en función a su red, tanto en planta interna[33] como externa[34]. Para lo cual, para dicho fin los operadores tienen que realizar lo siguiente:

   - Implementar adecuados mecanismos o sistemas de control de acceso en las puertas internas y externas.
   - Establecer medidas para la identificación del personal autorizado, así como sus niveles de acceso[35].
   - Los operadores que sólo presten el servicio público de distribución de radiodifusión por cable, y que no brinden servicios de valor añadido soportados en la red de cable, o servicios convergentes de telefonía fija y/o

[32] Cuando el secreto de las telecomunicaciones esté vinculado a la seguridad nacional, los operadores implementarán las medidas y procedimientos que fueran dispuestas por el MTC o la autoridad competente.

[33] Conjunto de equipos e instalaciones que se ubican dentro de la edificación que alberga la central, cabecera o nodo del servicio de telecomunicaciones. Incluye los equipos de los sistemas de conmutación, sistemas de transmisión y sistemas informáticos (base de datos, aplicativos, procesos.).

[34] Conjuntos de construcciones, cables, instalaciones, equipos y dispositivos que se ubican fueran de los edificios de la planta interna hasta el terminal de distribución. Será aérea, cuando los elementos están fijados en postes o estructuras, y, será subterránea, cuando los elementos se instalan en canalizaciones, cámaras ductos y conductos.

[35] En el caso de planta interna, se empleará tarjetas magnéticas y/o detectores de huella digital u otros identificadores. Para los operadores que sólo presten el servicio público de distribución de radiodifusión por cable sin valor añadido, podrán emplear otros mecanismos distintos a lo señalado.

acceso a Internet, podrán emplear otros mecanismos a fin de dar cumplimiento a esta obligación.

- Contar con un Manual Interno de procedimientos de seguridad, que sea de conocimiento del personal, lo cual será difundido mediante charlas de orientación, afiches, recordatorios, entre otros.

- Establecer medidas de incentivos al personal, con la finalidad de que cumplan con el referido Manual Interno.

2) Los operadores están obligados a resguardar la planta interna[36] y externa[37], implementando las medidas necesarias, para ello deberán comprender a los componentes físicos y/o lógicos que pudiesen facilitar la violación del secreto de las telecomunicaciones o el acceso a datos personales protegidos.

3) Identificar los ambientes internos y externos (oficinas, edificios, perímetros) que requieran protección y seguridad. Dichos ambientes deberán tener solidez física, asimismo no podrán contar con zonas que puedan derribarse con facilidad y permitir su acceso.

---

[36] Sobre las medidas de seguridad se aplicará lo siguiente:
- Los sistemas de conmutación y transmisión, en función a la red, contarán con mecanismos de protección y seguridad.
- Los equipos informáticos empleados para los procesos de facturación, tasación, bases de datos, entre otros, contarán con contraseñas de acceso, firewalls, software de detección y reparación de virus y software de protección contra códigos maliciosos, entre otros.

[37] En cuanto a las medidas de seguridad aplicables tenemos:
- Los armarios, contarán con mecanismos de seguridad, tales como candados con clave, candados con llave, platinas de seguridad con cerradura, entre otros.
- Las cajas de distribución contarán con mecanismos de seguridad, tales como cerraduras con llave, entre otros.
- Las cámaras deberán contar con mecanismos de seguridad tales como soldadura de tapas, contratapas, seguridad neumática, tapas especiales con grava, entre otros.
- Los repartidores principales (MDF), de ser el caso, y los recintos empleados para éstos, contarán con mecanismos de seguridad.
- Las estaciones base contarán con mecanismos de seguridad.
- Los armarios, contarán con mecanismos de seguridad, tales como candados con clave, candados con llave, platinas de seguridad con cerradura, entre otros.
- Las cajas de distribución contarán con mecanismos de seguridad, tales como cerraduras con llave, entre otros.
- Las cámaras deberán contar con mecanismos de seguridad tales como soldadura de tapas, contratapas, seguridad neumática, tapas especiales con grava, entre otros.
- Las estaciones base contarán con mecanismos de seguridad.

4) Emplear tecnología que brinde seguridad a la red, a través de mecanismos tales como autenticación, control de conexión de red y cifrado en los sistemas principales, bajo su control[38].

5) Implementar mejoras respecto a la seguridad física, infraestructura de red, seguridad de información y sistemas de sus redes, según corresponda al servicio que presta.

6) Como en toda empresa, se debe establecer pautas para el personal que labora, en el caso de los operadores, debido al tema de seguridad sus políticas laborales deberán tener un marco especial. Al respecto, la norma materia de comentario establece una serie de lineamientos que obligatoriamente deben seguirse[39]:

   - Celebrar acuerdos de confidencialidad con su personal y con terceros, sea que participe en la gestión comercial u operativa del servicio, y/o que tengan acceso a la planta externa o interna de las empresas operadora.

     En ese sentido, se debe prever que todo el personal se obliga a no divulgar cualquier información que pudiera facilitar o coadyuvar a la vulneración del secreto de las telecomunicaciones, aún después de extinguido el vínculo laboral o contractual; así como las consecuencias civiles y penales derivadas de su incumplimiento. Cabe indicar que la norma, si bien omite mencionar sobre la protección de datos personales, se sobreentiende que los operadores deben incluir este aspecto en los acuerdos de confidencialidad.

   - Cuando los operadores de telecomunicaciones celebren contratos con terceros, se debe exigir a éstos que suscriban acuerdos de confidencialidad con su personal que acceda a la planta interna o externa del operador, quien debe verificar dicho cumplimiento.

[38] Están exceptuadas de cumplir con ésta obligación, los operadores que presten exclusivamente el servicio público de distribución de radiodifusión por cable sin valor añadido.

[39] Estos lineamientos también son aplicables para estos casos:
- Cuando se trata de la protección de información contenida en los recibos de servicio telefónicos, como requerimiento de pago y otro comprobante de pago; así como información referida a la existencia de la comunicación y el historial de pago de abonado.
- Cuando se protege la información contenida en los contratos de abonado y en los contratos celebrado para la adquisición, de arrendamiento u otra modalidad de provisión de equipos terminales.

- Adoptar medidas de seguridad en la planta interna, y demás ambientes, desde donde se pueda acceder a esta información.

7) Realizar monitoreos[40], independientemente a las acciones de control que realicen periódicamente estos operadores, a fin de verificar el cumplimiento de las medidas y procedimientos adoptados, destinados a salvaguardar el secreto de las telecomunicaciones y proteger los datos personales, en la forma siguiente:

   - Tratándose de la Planta Interna, los monitoreos se realizarán conforme a lo que disponga la Dirección General de Control del MTC.

   - En el caso de la Planta Externa, los monitoreos se efectuarán sobre muestras, observando las disposiciones que emita la Dirección General de Control.

8) En caso que se logre identificar indicios o registrar antecedentes de vulneración a la seguridad implementada, se deberá adoptar medidas de seguridad adicionales que permitan minimizar dicho riesgo o amenaza.

2.6 Informes de los operadores de telecomunicaciones

En el informe anual que deberán presentar los operadores al Ministerio de Transportes y Comunicaciones, sobre las medidas adoptadas en el año anterior y las que se proyectan implementar durante el año en curso, para salvaguardar el secreto de las telecomunicaciones y la protección de datos, tienen que indicar lo siguiente:

1) La relación, contenido y descripción de las medidas implementadas; en especial, las destinadas para la seguridad y protección que son inherentes e implícitas de la tecnología implementada en su red y, en su caso, las medidas de seguridad de extremo a extremo implementadas, bajo su control.

[40] Los registros de los citados monitoreos, tanto de planta interna como externa, estarán a disposición de los inspectores autorizados de la Dirección General de Control.
Por su parte, los operadores que brinden de manera exclusiva el servicio de televisión por cable sin valor añadido realizarán estos monitoreos semestralmente.

2) Relación y contenido de las medidas implementadas para mantener la confidencialidad de la información personal que le hubiere sido proporcionada por sus abonados con quiénes mantienen o han tenido relación comercial.

3) Relación y contenido de las medidas internas implementadas para salvaguardar la seguridad de la red pública de telecomunicaciones, tanto en planta interna como externa. Tratándose de la infraestructura de planta externa, se incluirá las medidas implementadas respecto de armarios o cajas terminales instaladas en inmuebles de particulares o áreas de dominio público.

4) El personal responsable a cargo de la implementación y supervisión de las medidas y procedimientos adoptados para salvaguardar el secreto de las telecomunicaciones y la protección de datos personales.

5) El personal, propio o de terceros[41], que por la naturaleza de sus funciones, tiene acceso a los ambientes en los que se encuentran instalados los sistemas que podrían ser utilizados para vulnerar el secreto de las telecomunicaciones y/o la protección de datos personales de los abonados y/o usuarios[42].

6) Relación de medidas adoptadas en coordinación con el MTC o con la entidad competente, para salvaguardar el secreto de las telecomunicaciones en interés de la seguridad nacional.

Las modificaciones que se produzcan después de presentado el informe ante el MTC, deberán ser comunicadas a la Dirección General de Control de manera semestral[43]. El cómputo de este plazo, se realizará a partir de la fecha de presentación del referido informe anual. Si la modificación se refiere al personal responsable de la implementación de las medidas y procedimientos, serán comunicadas al MTC, al finalizar la primera o segunda quincena de cada mes, según el período en el que se produzca el cambio. En el caso que la modificación

[41] Éste es un agregado en relación a la Directiva derogada, que no contemplaba que un operador pudiese utilizar la tercerización para brindar sus servicios de telecomunicaciones.

[42] Están incluidas las personas naturales y/o jurídicas que, en ejecución de una relación contractual, prestan servicios al operador de telecomunicaciones.

[43] En la Directiva derogada se establecía como plazo para la comunicación, quince días calendarios siguientes de producida la modificación, lo cual elevaba los costos de las operadoras.

corresponda al personal que tiene acceso a los ambientes de los operadores, la comunicación se realizará, a más tardar, el último día hábil del mes, en el que se genere dicho cambio. Finalmente, la norma refiere que el MTC podrá solicitar a los operadores, cualquier información adicional a la que remiten en forma anual

2.7 Controles por parte del Ministerio de Transportes y Comunicaciones.

Las inspecciones a los operadores serán realizadas por la Dirección General de Control del MTC, a través de sus inspectores acreditados para dicho fin, quienes entregarán al representante del operador, un oficio expedido en la fecha por el Director General de Control, que deberá indicar la materia de la inspección, el nombre y otros datos de identificación de los inspectores autorizados.

Las inspecciones serán realizadas sin previo aviso[44] en cualquier día y hora, dentro del horario laborable del operador de telecomunicaciones, sin necesidad que para ello medie una denuncia de violación al secreto de las telecomunicaciones o de inobservancia a la norma que cautela la protección de los datos personales.

La norma permite que en casos excepcionales, la Dirección General de Control pueda realizar inspecciones fuera del horario laboral establecido por los operadores. El problema de este aspecto de la norma, es que la supuesta excepcionalidad podría derivar en algo rutinario, dado que deja un alto margen de discrecionalidad al ente inspector, lo cual podría llegar afectar el principio de libertad de empresa e, incluso, los derechos laborales de los trabajadores del la empresa operadora, por cuanto un procedimiento de inspección podría requerir de la presencia del personal autorizado fuera de su horario de trabajo. Consideramos que debió indicarse taxativamente los supuestos de excepción, en respeto al principio de legalidad administrativa.

El objeto de la inspección es la verificación del cumplimiento de las obligaciones por parte del operador para salvaguardar el secreto de las telecomunicaciones y la protección de datos personales, de las que se ha hecho mención en los numerales precedentes de este estudio.

[44] En la norma derogada las visitas inspectivas se comunicaban con 48 horas de anticipación, indicando las instalaciones objeto de la visita, día, hora y relación del personal designado para la inspección.

Durante la inspección el operador designará a los responsables que estarán presentes e instruirá al personal que tenga acceso a los ambientes donde están instalados los sistemas que sirven de soporte para salvaguardar los derechos constitucionales que motivan la expedición de la norma que se comenta, así como al personal encargado de implementar y supervisar las medidas y procedimientos adoptados, para que colabore con la labor de los inspectores, quienes levantarán un acta donde consignarán las medidas y procedimientos verificados, incluyendo las observaciones que formulen los representantes de la operadora. El acta deberá ser suscrita por el inspector y los responsables designados para intervenir en el procedimiento de inspección, y en ausencia de éstos, con quien se encuentre en el momento de la inspección.

Cuando se trate de inspeccionar la Planta Externa, se podrá verificar el interior de los elementos de red que se encuentren protegidos por las medidas de seguridad de acceso implementadas por el operador de telecomunicaciones; para tal efecto, dicho operador deberá asegurar la presencia del personal que posea los dispositivos o información que permitan el acceso a los referidos elementos.

Los inspectores podrán intervenir a cualquier persona que se encuentre realizando actividades en la planta externa del operador de telecomunicaciones, solicitando que se identifiquen y corroborarán de manera inmediata sus datos, contrastándolos con la información proporcionada por este operador, si es parte del personal que el operador ha autorizado y comunicado al MTC, para el cumplimiento de esta labor inspectiva se podrá requerir del apoyo de la fuerza pública.

Si en el marco de una inspección el personal de la Dirección General de Control, advirtiera la presunta comisión de una infracción referida a la vulneración al secreto e inviolabilidad de las telecomunicaciones o la protección de datos personales, independientemente de las acciones administrativas a que hubiera lugar, comunicará dichos hechos al Ministerio Público, para la adopción de las acciones correspondientes de acuerdo a su competencia[45].

[45] En la Directiva derogada, se permitía que el MTC otorgara un plazo prudencial a la empresa operadora a fin que mejore las medidas adoptadas.

El incumplimiento de las obligaciones establecidas en los numerales 10, 11.2, 11.3, 11.4 y 12 de la Resolución, se sujetan al régimen de infracciones y sanciones establecido en la Ley de Telecomunicaciones y su Reglamento.

2.8. Responsabilidades por incumplimiento de obligaciones.

A fin de brindar una mayor protección a este derecho, en el plano administrativo, se han establecido sanciones ante las infracciones que puedan cometer las empresas al incumplir su deber de protección de los datos personales.

En ese sentido, el artículo 258º inciso 1) del Reglamento, señala que constituye infracción muy grave, el incumplimiento de las obligaciones referidas a la protección de datos personales. Por su parte, el artículo 88° inciso 10 de la Ley de Telecomunicaciones, tipifica como falta grave, negarse a facilitar información relacionada con el servicio, a la autoridad de telecomunicaciones. Esta infracción, en lo concerniente a la obligación de salvaguardar el secreto de las telecomunicaciones y la protección de datos personales, tiene los siguientes alcances de conformidad con lo estipulado por el numeral 4 del artículo 261° del Reglamento:

a) No presentar al Ministerio la información prevista en la normativa dentro del plazo fijado.

b) Presentar la información a que se refiere el literal precedente de manera incompleta, siempre que no cumpliera con subsanar la omisión en el plazo otorgado por el Ministerio.

c) No presentar al Ministerio las modificaciones que se produzcan en relación a la información alcanzada dentro de los plazos previstos en la normativa.

d) Presentar la información de los referidos cambios de manera incompleta; siempre que no cumpliera con subsanar la omisión dentro del plazo otorgado por el Ministerio.

En lo relativo a las sanciones, los artículos 90° y 91° de la Ley, establecen que las infracciones tipificadas como muy graves y graves, se sancionan con multa[46], que fluctuará en el primer caso, entre treinta y cincuenta unidades impositivas tributarias (UIT), mientras que en el segundo será entre 10 y 30 UIT. Adicionalmente, dependiendo de la gravedad de la infracción, la autoridad administrativa puede ordenar el decomiso de los equipos y la revocación temporal o definitiva de la concesión o autorización[47].

Aparte de las responsabilidades administrativas antes descritas, también incurrirían en responsabilidad penal, las personas naturales que laboran en las empresas de telecomunicaciones y que vulneren la protección de los datos personales. En este caso, se estaría cometiendo el delito de violación del secreto profesional, tipificado en el artículo 165°[48] del Código Penal peruano de 1991.

Otro delito que puede cometerse, sea que se labore o no en una empresa de telecomunicaciones, pero que implique una vulneración de datos personales relacionados con el derecho a la intimidad, se tipifica en el artículo 157°[49] del acotado Código Penal.

---

[46] De acuerdo a esa norma, el pago de la multa no importa ni significa la convalidación de la situación irregular, debiendo el infractor cesar de inmediato los actos que dieron lugar a la sanción.

[47] Esta última sanción, puede ejecutarse anticipadamente como medida cautelar de conformidad con lo establecido en el artículo 96° de la Ley.

[48] "***Artículo 165°.- Revelación de información sujeta a secreto profesional.***
El que, teniendo información por razón de su estado, oficio, empleo, profesión o ministerio, de secretos cuya publicación pueda causar daño, los revela sin consentimiento del interesado, será reprimido con pena privativa de libertad no mayor de dos años y con sesenta a ciento veinte días multa."

[49] *"**Artículo 157°.- Organización y empleo abusivo de archivos.***
El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas, será reprimido con pena privativa de libertad no menor de uno mi mayor de cuatro años.
Si el agente es funcionario o servidor público y comete el delito en ejercicio del cargo, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al artículo 36°, incisos 1, 2 y 4."

3. CONCLUSIONES.

1) Existe a nivel constitucional en el Perú, una protección sobre los datos personales, mediante el artículo 2° inciso 6 de la Constitución Política de 1993; aunque no hay una norma de desarrollo que permita una mayor eficacia en la protección de ese derecho fundamental.

2) Existen algunas normas dispersas en el ordenamiento jurídico peruano, que regulan en casos especiales, sobre la protección a los datos personales, como sucede en el ámbito privado, con Ley N° 27849, que regula el suministro que efectúan las centrales privadas de información de riesgos; y en el sector público, con el Decreto Supremo N° 043-2003-PCM, que regula la Ley de Transparencia y Acceso a la Información Pública.

3) En el ámbito de las telecomunicaciones en el Perú, la protección sobre los datos personales se reconoce expresamente a partir del artículo 13° del Reglamento de la Ley de Telecomunicaciones, aprobado por el Decreto Supremo Nº 020-2007-MTC.

4) La Resolución Ministerial Nº 111-2009-MTC/03, viene a significar un importante avance respecto a la regulación sobre la obligación que tienen los operadores, para proteger los datos personales de sus usuarios y/o abonados, así como salvaguardar el secreto de las telecomunicaciones, al establecerse las pautas sobre las medidas y procedimientos de seguridad a implementarse.

5) Sin embargo, esta Resolución Ministerial adolece de algunas omisiones, principalmente, en el ámbito de protección, que podrían originar un conflicto entre los Operadores de los Servicios Públicos de Telecomunicaciones con los usuarios de sus servicios y con el Poder Judicial, lo cual afectaría la seguridad jurídica que deben brindar estos operadores en la prestación de estos importantes servicios de telecomunicación.

6) Es una característica de la normatividad peruana, aunque aún no plasmada a nivel constitucional, que la autorización para la obtención de datos personales de los

archivos, se realice mediante autorización del titular de la información o por autorización judicial.

7) Otra característica de la normatividad peruana, es que existe el deber de reserva de quienes administran las bases de datos, tanto sean personas jurídicas como naturales e incluyen a los empleados de éstos, originándose responsabilidades de índole administrativa y penal.