



Association Internationale de Droit des Assurances

CUESTIONARIO DE LA SECCIÓN ARGENTINA
PARA EL XIIº CONGRESO MUNDIAL DE DERECHO DE SEGUROS
BUENOS AIRES 2006

**LA INFLUENCIA DE LOS AVANCES CIENTIFICOS Y TECNOLOGICOS
EN LOS SEGUROS DE PERSONAS**

Portugal

A.) Introducción

A1. Si, siempre y cuando se cumplan los requisitos legales que rigen los contratos de seguro. La Directiva 2002/65/EC del Parlamento Europeo y del Consejo, del 23 de septiembre de 2003 sobre la comercialización a distancia de los servicios financieros al consumidor debería ser incluida en una ley nacional en el futuro próximo.

A2. Es posible, siempre y cuando se registren en formato duradero (que permita que la información enviada al consumidor sea almacenada y permita fácil acceso en el futuro en caso de ser requerida a los fines para los cuales fue destinada y pueda ser reproducida sin alteraciones).

A3. Es posible en algunos sitios, al menos en el caso de ciertos tipos de contratos (automóvil, viaje, seguro de vivienda), siempre que se ofrezca acceso al sitio reservado (por ej. Allianznet). En teoría es perfectamente posible.

A4. Las implicancias de esta pregunta no son claras. Antes de ser completado, el formulario de la propuesta no se considera confidencial ya que no contiene datos personales. El formulario pertenece a la entidad que lo emitió.

A5. Si, la Ley de Delitos Informáticos (Law on Computer Crime) Decreto-Ley N° 109/91 del 17 de agosto de 1991, modificada por el Decreto-Ley N° 323/2001 del 17 de diciembre de 2001).

Artículo 193

Abuso informático

1 – Toda persona que creare, mantuviere o utilizare archivos computarizados que incluyan datos que identifiquen personas y se refieran a posturas políticas, filosóficas o creencias religiosas, pertenencia a partidos políticos o sindicatos, grupos religiosos o a información personal u origen étnico será penado con sentencia de hasta 2 años o multa de hasta 240 días.

2 – Cualquier intento de cometer el delito descrito arriba también será penado.

A6. La privacidad del correo electrónico está cubierta por la privacidad de las comunicaciones y la protección de la vida privada. La Ley de Protección de los Datos Personales (Ley N° 67/98 del 26 de octubre de 1998) establece el procesamiento y transferencia libre de los datos personales, y se incluye en el sistema legal portugués la Directiva 95/46/EC del Parlamento Europeo, del 24 de octubre de 1995, sobre la protección de las personas en relación al procesamiento de los datos personales y la libre circulación de dichos datos.

Los delitos cometidos en este contexto son los siguientes:

Artículo 194

Violación de la correspondencia o las telecomunicaciones

1 – Toda persona que, sin autorización, abriere un paquete, carta o cualquier otro tipo de comunicación escrita sellada y dirigida a otra persona o que descubriere su contenido por algún medio técnico, o que de alguna otra manera evitase que dichos objetos llegaran a su destinatario, será penado con sentencia de prisión de hasta 1 año o multa de hasta 240 días.

2 – La misma pena será aplicada a aquella persona que, sin autorización, interfiriere en el contenido de una telecomunicación o descubriere su contenido.

3 – Toda persona que, sin autorización, revelare el contenido de una carta, paquete o comunicación escrita sellada o telecomunicación mencionada en el punto anterior será penada con sentencia de prisión de hasta 1 año o multa de hasta 240 días.

Artículo 384

Violación de la confidencialidad de la correspondencia o las telecomunicaciones

Cualquier empleado de los servicios postales, de telegrafía, telefonía o telecomunicaciones quien, sin debida autorización:

Suprimiere o retirare una carta, parcela, telegrama u otro tipo de comunicación confiada a dichos servicios a los cuales tuviera acceso debido a la naturaleza de su tarea;

Abriere una carta, parcela u otro tipo de comunicación al cual tuviere acceso debido a la naturaleza de su trabajo o descubriere su contenido sin abrirlo;

Revelare a terceros cualquier tipo de comunicación entre particulares efectuada por correo, telégrafo, teléfono u otra forma de comunicación brindada por estos servicios, de las que tuviera conocimiento debido a la naturaleza de su trabajo;

Registrare o revelare a terceros el contenido total o parcial de las comunicaciones mencionadas o permitiera su escucha o acceso a su contenido; o

Permitiere o facilitare cualquiera de las situaciones descritas en los puntos anteriores; será penado con sentencia de prisión de entre 6 meses a 3 años o una multa no inferior a los 60 días.

A7. Nada dispone la ley para prevenirlo o limitarlo.

A8. Nada dispone la ley para prevenirlo o limitarlo.

A9. Los datos no obtenidos por el ISP. El APS recaba esta información para todas las pólizas a excepción de los seguros de vida, aunque no hace distinción alguna entre los tipos de pólizas.

A10. Los contratos de seguro están exentos del pago del IVA.

Código de IVA

PARTE I

Transacciones locales exentas

Artículo 9

1 – Las siguientes actividades se encuentran exentas de impuestos:

29 – Seguros y reaseguros, además de los servicios relacionados prestados por los brokers e intermediarios de seguros;

PARTE II

Importaciones exentas

Artículo 13

1 –Las siguientes actividades se encuentran exentas de impuestos:

a) La importación final de bienes, cuya provisión se encontrare exenta en el territorio del país;

B.)

B1. Si

B2. En principio, si. Las pocas modificaciones, como el derecho a la libre resolución en el caso de los contratos a distancia (equivalente al derecho de renuncia en los seguros de vida), tienen como fin proteger al consumidor.

B3. En principio, si. Ver respuesta anterior.

B4. Si.

B5. Depende de su significado exacto. Si implica que los interesados pueden celebrar un contrato a través de Internet, la respuesta es si, a excepción de los contratos firmados por autoridades públicas (por ej. por instrumento público). Si implica que los contratos celebrados a través de Internet eliminan la necesidad de que las partes contratantes queden sujetas a las obligaciones establecidas por ley, la respuesta es no.

B6. Los documentos electrónicos son equivalentes a los documentos escritos:

*Decreto-Ley N° 7/2004 del 7 de enero
(traspone la Directiva EC sobre Comercio Electrónico)*

Artículo 26

Formato

1 – Las declaraciones emitidas por mecanismos electrónicos cumplen los requisitos legales cuando presentan un formato que ofrece las mismas garantías de confiabilidad, comprensión y conservación.

2 – Un documento electrónico es equivalente a un documento firmado si cumple los requisitos legales establecidos para el caso de la firma y certificación electrónica.

C.)

C1. El formato escrito sigue siendo obligatorio, aunque no debe presentarse en papel necesariamente. Sin embargo, debe ser presentado en un formato duradero (que ofrezca las mismas garantías de confiabilidad, comprensión y conservación que el formato papel).

C2. El Instituto das Tecnologias da Informação na Justiça (Instituto de Tecnología de la Información Judicial) es un organismo público que certifica a los organismos certificantes. El organismo certificante es una persona física o jurídica que produce o entrega los medios para crear o verificar firmas, emite certificados, garantiza que sean publicados y brinda otros servicios relacionados con la firma electrónica. El certificado es un documento electrónico que relaciona los datos que verifican la firma con su dueño y, así, se confirma la identidad del dueño.

Condiciones para la certificación:

(Decreto Ley N° 290-D/99 y Decreto Ley N° 234/2000 del 25 de septiembre de 2000)

Artículo 28

Emisión de certificados acreditados

1 – Ante solicitud o en representación de una persona física o jurídica, el organismo de certificación emite los datos para la creación y verificación de una firma o, en caso de

solicitud, pone a disposición los medios técnicos para permitirlo y debe, en todo momento, verificar por los medios legales adecuados y seguros, la identidad y, si correspondiere, las facultades de representación del solicitante.

2 – Ante solicitud del propietario, el organismo de certificación emite uno o más ejemplares del certificado o un certificado complementario.

3 – El organismo de certificación debe tomar las medidas adecuadas para evitar cualquier falsificación o modificación de los datos contenidos en los certificados y debe garantizar el cumplimiento de todas las normas y reglamentos correspondientes, empleando personal calificado para este fin.

4 – El organismo de certificación entrega a los propietarios de los certificados toda la información necesaria para utilizar las firmas de manera correcta y segura:

a) Las obligaciones del propietario del certificado y del organismo de certificación;

b) Los procedimientos para agregar y verificar la firma;

c) La conveniencia de volver a firmar documentos en los que la firma ya ha sido estampada, cuando circunstancias técnicas lo justifican.

5 – El organismo de certificación organizará y mantendrá registros informáticos actualizados de todos los certificados emitidos, suspendidos o revocados, que estarán a disposición de cualquier persona para su consulta, incluso por medio de la telecomunicación, y serán protegidos contra cualquier tipo de alteración no autorizada.

C3. Si.

Decreto Ley N° 290-D/99

Artículo 6

Transmisión de documentos electrónicos

3 – La transmisión, a través de las telecomunicaciones, de documentos electrónicos en los cuales figurare una firma electrónica para garantizar su recepción es equivalente a la recepción de un correo certificado y, en caso de que el receptor envíe un mensaje de confirmación al emisor en el mismo formato, es equivalente a un envío postal con entrega certificada.

D.)

D1.

D2.

D3. Si.

Decreto Ley N° 290-D/99 del 2 de agosto, modificado por el Decreto Ley N° 62/2003 del 3 de abril (ley sobre documentos electrónicos y firmas electrónicas)

Artículo 7

Firmas electrónicas acreditadas

1 – Una firma electrónica acreditada estampada en un documento electrónico es equivalente a la firma manuscrita en un documento de papel y presupone lo siguiente:

a) La persona que estampó la firma electrónica acreditada es el propietario de la firma o el representante de la persona jurídica que es propietaria de la firma electrónica acreditada, con amplias facultades de representación;

b) La firma electrónica acreditada fue estampada con la intención de firmar el documento electrónico;

c) El documento electrónico no ha sido modificado desde que la firma electrónica acreditada fuera estampada.

2 – La firma electrónica acreditada debe remitir sin equivocación alguna a una única persona física o jurídica y al documento en el cual ha sido estampada.

3 – El agregado de una firma electrónica acreditada sustituye, a los fines legales, cualquier sello, timbre, etiqueta comercial u otra marca identificatoria del propietario.

4 – El agregado de una firma electrónica acreditada en un documento que, a la fecha en la cual la firma fue estampada, ha expirado, ha sido revocado o suspendido o no respeta los términos y condiciones de su emisión, es equivalente a un documento no firmado.

D4. Si.

Decreto Ley N° 290-D/99 Artículo 3

Formato y condición como evidencia

1 – Los documentos electrónicos cumplen los requisitos legales del formato escrito cuando su contenido es representado como declaración escrita.

2 – Cuando la firma electrónica acreditada por parte de un organismo de certificación acreditado ha sido estampada, los documentos electrónicos cuyos contenidos cumplen la descripción del punto anterior tienen la misma condición de prueba que el documento privado firmado conforme las disposiciones del Artículo 376 del Código Civil.

3 – Cuando la firma electrónica acreditada por un organismo de acreditación ha sido estampada, los documentos electrónicos cuyo contenido no pueden ser representados como declaración escrita tienen la misma condición de prueba que la establecida en el Artículo 368 del Código Civil y el Artículo 167 del Código de Procedimiento Penal.

4 – Las disposiciones de los puntos anteriores no limitan el uso de otros medios de prueba de la autoría e integridad de los documentos electrónicos, incluyendo otras formas de firma electrónica, siempre y cuando estos medios son adoptados por ambas partes en un acuerdo válido sobre evidencia o cuando son aceptadas por la persona a la cual se dirige el documento.

5 – No obstante lo dispuesto en el punto anterior, el valor de prueba de los documentos electrónicos no estampados con una firma electrónica acreditada por un organismo de certificación acreditado será considerado conforme los términos de la ley general.

D5.

En general, existen dos tipos de algoritmos criptográficos:

- simétrico, o convencional, que utiliza una única clave para encriptar o decriptar.
- asimétrico o claves públicas, en cuyo caso se utilizan dos claves diferentes y matemáticamente relacionadas (Pública y privada).

Algo que ha sido encriptado por una única clave SOLO puede ser descryptada por la otra.

En otras palabras:

Toda información codificada por una clave privada sólo puede ser decodificada por la clave pública correspondiente (del par).

Toda información codificada por una clave pública sólo puede ser decodificada por la clave privada correspondiente (del par).

Nota: La Clave Privada es personal e intransferible y debería contar con medidas de protección adecuadas.

Para crear una firma digital, el emisor del mensaje debe, en primer lugar, generar una versión del mensaje (una versión reducida de, por ejemplo, 160 bits) conocida como código hash o código de mensaje. Este código, generado por algoritmos públicos (SHA-1, MD5, etc) es único para el texto original. En caso de alterar el texto original, aun de manera mínima, el código generado será completamente diferente.

El emisor crea una firma digital al firmar consecutivamente (codificar) el código de mensaje hash con su clave privada.

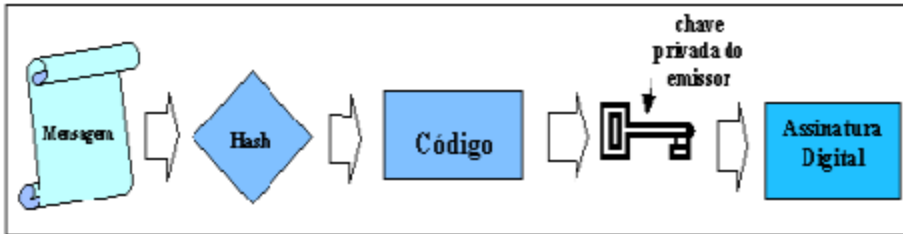


Figura 1 –Procedimiento automático para obtener un mensaje firmado digitalmente.

Para evitar que cualquier persona diferente al receptor designado pueda tener acceso al contenido de un mensaje o, en otras palabras, para garantizar la confidencialidad en la transmisión de la información, el emisor agrega esta firma digital al mensaje original que, a su vez, codifica con la clave pública del receptor. Así se genera un documento electrónico digital con una firma digital.

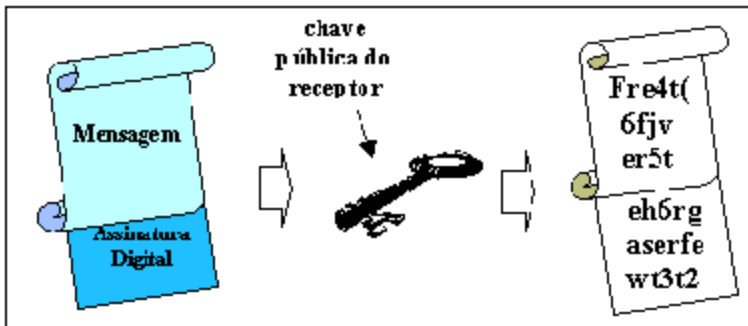


Figura 2 –Procedimiento para codificar mensajes firmados digitalmente.

Al recibir el mensaje, el receptor abre el texto con su clave privada. Para obtener la firma digital original en un formato legible, el receptor decodifica el código hash con la clave pública del emisor (Valor A). Para verificar la firma digital y la integridad de la información, el receptor crea un código hash para el mensaje original recibido (Valor B) y compara este código con el que obtuvo al descifrar la firma digital (Valor A). Si el receptor puede validar la firma digital utilizando la clave pública del emisor, puede garantizar que el mensaje fue enviado por el propietario de la clave y que no ha sido modificado durante la transmisión.



Figura 3 –Procedimiento para validar mensajes firmados digitalmente

Notas:

Mensagem: Mensaje

Código: Código

Chave privada do emissor: clave privada del emisor

Chave pública do emissor: clave pública del emisor

Assinatura digital: firma digital

Sim: si

Não: No

Para garantizar que el par de claves (pública y privada) pertenece a un emisor determinado, se utilizan los Certificados Digitales, emitidos por un tercero de confianza.

Antes de que las dos partes intercambien información encriptada mediante el uso de la clave pública, cada uno puede tomar la decisión de autenticar la identidad de la otra parte. Por ejemplo, los emisores pueden querer saber que realmente están tratando con el receptor elegido. Los receptores también querrán asegurarse de la identidad del emisor y de la precisión de la información que se intercambia.

Una manera de asegurar la autenticidad de las dos partes es recurrir a los servicios de un tercero que emite y regula la administración de los servicios de certificación digital.

Un certificado digital es un documento firmado digitalmente y emitido por un tercero acreditado y de confianza conocido como organismo de certificación. Utilizando métodos públicos y de clara definición, el organismo de certificación regula la certificación a través de la emisión, renovación y cancelación de certificados aprobados en forma particular.

Para crear un certificado digital, el organismo de certificación genera un código hash que, entre otros datos, incluye información sobre la identidad del usuario y su clave pública. El organismo de certificación "firma" esta información con su clave privada, con lo que crea un código hash encriptado. Esta información se incluye en el certificado que se emite. Si la información sobre la identidad del usuario o la clave pública contenida en el certificado digital sufre alguna modificación, el certificado queda invalidado.

Para confirmar la autenticidad del certificado digital, el receptor:

- Regenera el código hash utilizando el mismo algoritmo e información utilizada por el organismo de certificación en la creación del código hash para el certificado en cuestión (Valor A).
- Decodifica el código hash incluido en el certificado digital utilizando la clave pública del organismo de certificación (Valor B).
- Compara los dos Valores (A y B) y, si son los mismos, el certificado será válido. De lo contrario, el certificado digital ha sido modificado y no es válido.

<http://www.multicert.pt/pergunta1.htm>

Estructura de los Certificados Digitales X.509 v3

La estructura de los certificados digitales administrados por MULTICERT incorpora el estándar X.509 v3, que permite adecuar los contenidos según extensiones adaptadas y definidas previamente (conforme los estándares PKCS#6 y PKCS#9). Así, se pueden incluir datos específicos del usuario y los niveles de criticidad con sus identificadores correspondientes (por ejemplo, identificación del domicilio de una persona, codificación de los niveles de acceso a la información o el contexto en el cual se utilizará el certificado).

Diagrama simple de un certificado digital X.509 v3 (sin extensiones del estándar v3)

Información básica

| | |
|--|---|
| Formato del certificado | versión 3 |
| Número de serie del certificado | 123456789 |
| Identificación del algoritmo de la firma EC | RSA con MD5 |
| Domicilio X.500 del emisor | C=PT,o=EC |
| Validez | desde=01/08/96, hasta=01/08/98 |
| Nombre X.500 del usuario | c=PT, o=organización, cn=João Silva + |
| Clave pública del usuario y método de encriptación | C.P.U. + RSA con MD5 |

Extensiones V3

| | | | |
|------|------------|-------|---|
| Tipo | Criticidad | Valor | domicilio, bit off/no crítico, Rua das Codornizes 183 |
| Tipo | Criticidad | Valor | uso, bit on/crítico, Válido sólo con firma digital |
| Tipo | Criticidad | Valor | Nivel de acceso, bit off/no crítico, 1- general |
| Tipo | Criticidad | Valor | |

(<http://www.multicert.pt/pergunta2.htm>)

Preguntas frecuentes: <http://www.multicert.pt/perguntas.htm#6>

E.) Acceso a bases de datos

E1. El acceso a las bases de datos es posible sólo conforme la ley de protección de datos o por orden judicial.

E2. Detección de delitos.

E3. Ver E1.

F.) Exclusiones en seguros personales

F1. No.

F2. No.

F3. No.

F4. No.

G.) Derecho de subrogación

G1. En general, no hay subrogación cuando la obligación del asegurador consiste en un valor preestablecido.

H.)

H1. El análisis de riesgo puede incluir pruebas de diagnóstico complementarias como los análisis de sangre y orina, endoscopías, radiografías, ecografías, biopsias, tomografía computada, resonancias magnéticas, pruebas de SIDA, electrocardiogramas y ecocardiogramas. Sin embargo,

estos análisis se realizan en casos específicos; no se observa un patrón general en el mercado.

H2. La ley sobre datos genéticos e información de la salud (Ley 12/2005 del 26 de enero de 2005) establece que la propiedad de este tipo de información pertenece a la persona afectada (Artículo 3).

La investigación del genoma humano (Artículo 16) cumple las normas generales sobre la investigación científica en el campo de la salud y debe respetar la confidencialidad sobre la identidad y las características de las personas evaluadas y garantizar que la comunidad científica tenga acceso libre a los datos resultantes.

La investigación del genoma humano está sujeta a la aprobación del comité de ética del hospital, la Universidad o unidad de investigación.

La investigación del genoma humano con participación de personas no puede realizarse sin antes obtener el consentimiento informado de los participantes, por escrito, una vez que se les hayan explicado sus derechos, la naturaleza y objetivos de la investigación, los procedimientos utilizados y el riesgo potencial que los mismos u otras personas pudieran correr.

H3. El artículo 11 de la ley 12/2005 establece el principio de no discriminación:

- Ninguna persona sufrirá perjuicio alguno a causa de una enfermedad o herencia genética.
- Ninguna persona será discriminada a causa de los resultados de evaluaciones de heterocigosidad, pruebas presintomáticas o pruebas genéticas de diagnóstico, incluyendo las evaluaciones realizadas para la obtención o mantenimiento del empleo, evaluaciones para la obtención de un seguro de vida o médico, acceso a la educación o aquellos estudios realizados en procesos de adopción, con participación del adoptado o de los padres adoptantes.
- Ninguna persona será discriminada por negarse a someterse a un examen genético, especialmente en relación a su derecho a recibir tratamiento médico o psicológico o a realizar una consulta genética.
- Se garantiza igual acceso a las consultas genéticas y exámenes genéticos, con debida excepción de aquellas poblaciones afectadas por una enfermedad o enfermedades genéticas determinadas.

Aunque todavía no ha sido transpuesta a la ley nacional portuguesa, la Directiva que implementa el principio sobre trato equitativo entre los hombres y las mujeres en el acceso y provisión de bienes y servicios (Directiva del Consejo 2004/113/EC del 13 de diciembre de 2004) debe ser considerada.

H4. Conforme las disposiciones de la Ley 12/2005, la información médica se refiere a la información sobre la salud que tiene como objetivo ser utilizada en la provisión de servicios de salud o tratamiento médico (Artículo 5).

“La historia clínica” se refiere a cualquier archivo, computarizado o de otra característica, que contenga información sobre la salud de un paciente o de su familia. Cada historia clínica debe contener toda la información médica disponible sobre la persona, con la condición de que dicha información sea ingresada por el médico que atiende a la persona o de que, bajo su supervisión, sea ingresada en una computadora por otro profesional que también tenga obligación de observar el secreto profesional en el contexto de las obligaciones específicas de cada profesión y el cumplimiento de las condiciones deontológicas correspondientes.

La historia clínica sólo puede ser consultada por el médico responsable de brindar atención médica a la persona involucrada y por otro profesional de la salud que se encuentre bajo su supervisión y estuviera sujeto a guardar el secreto profesional y sólo cuando fuera estrictamente necesario y no comprometa la investigación epidemiológica, clínica o genética que pudiera conducirse, con la excepción de las investigaciones sobre el genoma humano, en virtud de las disposiciones del Artículo 16 de la Ley 12/2005 mencionado en la respuesta H2.

H5. El procesamiento de la información sobre la salud está cubierta por las disposiciones del Artículo 4 de la Ley 12/2005 bajo los siguientes términos:

- Los responsables del procesamiento de la información sobre la salud deben tomar las medidas necesarias para proteger su confidencialidad, garantizar la seguridad de las instalaciones y el equipamiento, controlar el acceso a esta información y, además, reforzar la necesidad de guardar el secreto profesional y brindar educación deontológica para todos los profesionales.

- Las unidades del sistema de salud deben evitar el acceso no autorizado de terceros a historias clínicas y sistemas de información que contengan datos sobre la salud, incluyendo copias de seguridad, y deben garantizar niveles adecuados de seguridad y cumplir con los requisitos legales sobre la protección de los datos personales, especialmente con el fin de evitar accidentes o la destrucción ilícita, alteración, diseminación o acceso no autorizado u otra forma ilícita de procesamiento de la información.

- La información sobre la salud sólo puede ser utilizada por el sistema de salud en circunstancias especiales que requieran una autorización por escrito del propietario de la información o su representante.

- El acceso a la información sobre la salud, en caso de ser anónima, debe ser autorizada a los fines de una investigación.

- Los sistemas que organizan la información sobre la salud deben ser administrados de manera que garanticen que la información sobre la salud o los datos genéticos queden separados de otro tipo de información personal mediante el establecimiento de diferentes niveles de acceso.

- Los sistemas de información deben ser administrados de manera que garanticen el procesamiento regular y frecuente de las copias de seguridad, a la vez que se garantice la confidencialidad establecida por ley.

H6. Políticas que contengan cláusulas cuyo fin sea evitar " el enriquecimiento injusto" .

La noción de " enriquecimiento injusto" , cuyo efecto acumulativo causa que una persona adquiera riquezas a expensas de otra sin justificación alguna, está establecida en el Artículo 473 del Código Civil Portugués.

Artículo 473 (Principios Generales)

1. Cualquier persona que, sin causa justa, se enriqueciere a expensas de otra deberá devolver la suma obtenida de manera irregular.

2. El objeto específico de la obligación de devolver, debido al enriquecimiento injusto, es aquello que fue recibido indebidamente o que fue recibido por una razón que ya no es válida o como resultado de un hecho que no puede ser verificado.

Por lo tanto, las pólizas establecen que, en caso de reclamo, una de las obligaciones del titular de la póliza frente al asegurador es informar la existencia de otras pólizas que cubren el mismo riesgo. Ello debería ser comunicado a todos los aseguradores junto con los nombres de los

demás aseguradores.

Si, a la fecha del reclamo, existieran otros contratos de seguro que cubren todas o algunas de las garantías aseguradas, se aplicará el contrato firmado en primer lugar. Los demás contratos de seguro sólo se aplicarán en caso de que el contrato de seguros previo no existiera, no fuera efectivo o no pudiera ser aplicado.

I.)

11. La Ley sobre información genética personal e información sobre la salud (Ley 12/2005 del 26 de enero) define el concepto de información sobre la salud y la información genética, la circulación de esta información y la intervención en el genoma humano dentro del sistema de la salud, así como las normas sobre la recolección y almacenamiento de productos biológicos con fines de evaluación o investigación.

Según las disposiciones de la Ley 12/2005, la información genética se refiere a lo siguiente:

- La información genética o información sobre la salud que incluye características hereditarias de una o más personas relacionadas entre sí o que comparten características de este tipo. La información derivada de evaluaciones parentales, estudios de cigosidad de mellizos y estudios de identificación genética con fines penales así como los estudios de mutaciones genéticas somáticas en cáncer se encuentran excluidos en esta definición.

- La información genética puede ser el resultado de evaluaciones genéticas biológicas moleculares o puede obtenerse como resultado de evaluaciones por imágenes, citogénesis, bioquímica o psicología o la simple recolección de información familiar registrada en un árbol genealógico o similar, que en sí mismo exprese la condición genética de una persona o de sus relaciones.

- La información genética pasa a ser de naturaleza médica sólo cuando tiene como fin ser utilizada en la provisión del cuidado de la salud o tratamiento médico en caso de necesidad de confirmar o eliminar un diagnóstico clínico, prenatal o de pre-implantación o en farmacogénesis. Por lo tanto, se excluye la información obtenida de pruebas para predecir la susceptibilidad ante enfermedades comunes y evaluaciones presintomáticas para enfermedades monogénicas.

- La información genética que no tiene implicancias inmediatas para la condición de la salud, como por ejemplo los resultados de exámenes de paternidad, estudios cigósicos de mellizos, los resultados de pruebas predictivas- con la excepción de pruebas genéticas para determinar la propiedad de la medicina –y de heterocigosidad, evaluaciones prenatales o de pre-implantación no pueden ser incluidas en las historias clínicas, salvo en casos de medicina genética, en cuyo caso se llevan registros por separado.

- En el caso de las historias clínicas para los casos o servicios de la medicina genética, no se permite acceso o consulta por parte de médicos, otros profesionales de la salud o personal de otros servicios dentro de la misma institución u otras instituciones del sistema de salud si contienen información genética sobre individuos sanos.

- La información genética debe quedar sujeta a medidas legislativas y administrativas de protección que refuercen los niveles de acceso, seguridad y confidencialidad.

- El uso de la información genética es un acto que involucra al propietario de esta información y

a su médico, y está sujeta a normas deontológicas sobre el secreto profesional de los médicos y otros profesionales de la salud.

- La existencia de cualquier vínculo laboral entre los médicos u otros profesionales de la salud y cualquier actividad comercial, incluyendo a las compañías de seguro, organismos profesionales o proveedores de bienes y servicios no justifica ningún tipo de reducción de la obligación de mantener la confidencialidad.

- Los ciudadanos tiene derecho a saber si las historias clínicas, archivos o cualquier tipo de dato médico o de investigación incluye información genética sobre ellos y sus familias y a saber el fin y los usos a los que dicha información está destinada como así también al plazo y la forma de almacenamiento.

12. El artículo 12 de la Ley 12/2005 establece las normas sobre la evaluación genética y el seguro:

- Las compañías de seguro no pueden solicitar ni utilizar ningún tipo de información genética con el fin de rechazar un seguro de vida o establecer primas más elevadas.

- Las compañías de seguro no pueden solicitar a sus clientes potenciales la realización de pruebas genéticas con el fin de otorgar un seguro de vida o salud u otros.

- Las compañías de seguro no pueden utilizar información genética obtenida de pruebas genéticas realizadas por clientes actuales o potenciales con el fin de otorgar un seguro de vida o salud u otros fines.

- Los aseguradores no pueden exigir o utilizar datos genéticos obtenidos o registrados en generaciones anteriores de los miembros de una familia con el fin de rechazar una póliza o establecer primas más elevadas o con otros fines.

13. La Ley 12/2005 (Artículo 11) establece el principio de no discriminación:

- Ninguna persona sufrirá perjuicio alguno a causa de una enfermedad o herencia genética.

- Ninguna persona será discriminada a causa de los resultados de evaluaciones de heterocigosidad, pruebas presintomáticas o pruebas genéticas de diagnóstico, incluyendo las evaluaciones realizadas para la obtención o mantenimiento del empleo, evaluaciones para la obtención de un seguro de vida o médico, acceso a la educación o aquellos estudios realizados en procesos de adopción, con participación del adoptado o de los padres adoptantes.

- Ninguna persona será discriminada por negarse a someterse a un examen genético, especialmente en relación a su derecho a recibir tratamiento médico o psicológico o a realizar una consulta genética.

- Se garantiza igual acceso a las consultas genéticas y exámenes genéticos, con debida excepción de aquellas poblaciones afectadas por una enfermedad o enfermedades genéticas determinadas.

14. El Artículo 11 (2) de la Ley 12/2005 establece que ninguna persona será discriminada a causa de evaluaciones de heterocigosidad, pruebas presintomáticas o pruebas genéticas de diagnóstico, incluyendo las evaluaciones realizadas para la obtención o mantenimiento del empleo, evaluaciones para la obtención de un seguro de vida o médico, acceso a la educación o aquellos estudios realizados en procesos de adopción, con participación del adoptado o de los padres adoptantes.

15. Como ya se ha mencionado, la Ley Portuguesa (Artículo 12 de la Ley 12/2005) prohíbe las pruebas genéticas en el caso de los solicitantes de seguros personales (Seguros de Salud y Vida).

Aun si no fuera el caso, la persona es la dueña de la información sobre la salud (Artículo 3 de la Ley 12/2005):

- La información sobre la salud, incluyendo cualquier dato registrado que fuera resultado de pruebas u otros exámenes complementarios, intervenciones y diagnósticos, pertenece al individuo involucrado y esta información será conservada en las unidades de cuidado de la salud. No podrá ser utilizada con ningún otro fin diferente al cuidado de la salud, estudios de la salud u otros fines establecidos por ley.

- El propietario de la información sobre la salud tiene el derecho, si así lo deseara, de ser informado sobre todos los registros médicos relacionados con su persona o de que esta información sea entregada a una persona designada por él, salvo en circunstancias excepcionales o justificadas en las que se demuestre de manera fehaciente que pudiera ser perjudicial.

- El acceso a la información de la salud será autorizado al propietario de esta información o aun tercero, con el consentimiento de la persona involucrada, a través de un médico debidamente calificado y elegido por el propietario de la información.

16. Los aseguradores no pueden conducir exámenes genéticos en aquellas personas que soliciten seguros de vida (Artículo 11, punto 2 de la Ley 12/2005).

17. Comprometido.

18. Los aseguradores no pueden conducir exámenes genéticos en aquellas personas que soliciten seguros de vida (Artículo 11 (2) de la Ley 12/2005) ni utilizar la información genética obtenida en exámenes genéticos previos sobre sus clientes actuales o potenciales con el fin de otorgar seguros de vida o de salud (Artículo 12 (3) de la Ley 12/2005).

19. Si así lo desearan, los titulares de pólizas podrán informar la realización de exámenes genéticos. Sin embargo, como este tipo de información está clasificada legalmente como información sobre la salud (Artículo 6 (1) y Artículo 4 (1) de la Ley 12/2005), se considera confidencial.

Los resultados de los exámenes genéticos son propiedad de la persona involucrada y, aun cuando autorizaran el acceso a terceros, no puede ser utilizada por los aseguradores como lo establece el Artículo 12 (3) de la Ley 12/2005.

En resumen, esta información no puede ser utilizada por los aseguradores en la práctica y, por lo tanto, no deben solicitarla.

110. Ver la respuesta a la pregunta anterior.

111. En nuestro mercado, los aseguradores no pueden realizar pruebas genéticas en aquellas personas que solicitan un seguro de vida (Artículo 11 (2) de la Ley 12/2005). El impacto de esta medida en cuanto a la producción de primas no ha sido objeto de estudio.

112. Comprometido.

113. En nuestra opinión, este caso, en teoría, constituye un contrato de seguro no válido, debido a inexactitudes u omisiones (Artículo 429 del Código Comercial Portugués).

Cualquier declaración inexacta, así como la falta de información de hechos o circunstancias conocidas para el titular de la póliza o para la persona responsable de tomar el seguro, que pudiera influir en la existencia del mismo contrato o de las condiciones que contiene, invalida la póliza.

En caso de que hubiera prueba de mala fe por parte del individuo que realiza las declaraciones, el asegurador tiene derecho a retener la prima.

Sin embargo, no se conocen casos de este tipo en concreto ya que se trata de información confidencial a la que el asegurador no tiene acceso. Aun cuando el asegurador tuviera acceso a esta información (suponiendo que se obtuvo autorización del titular de la póliza) no tendría posibilidad de hacer uso de ella (Artículo 11 (2) de la Ley 12/2005).

114. Ver respuesta anterior.

Tucumán 994, 3er.piso. (1049) Ciudad Autónoma Buenos Aires, Argentina. Telephone and fax.: (54-11) 5218-0044 (toll lines)
VIA INTERNET: [E - MAIL claudiospeyer@speyer-mariani.com](mailto:claudiospeyer@speyer-mariani.com)