ISSN 0123-1154 (IMPRESO)
ISSN 2500-7556 (EN LÍNEA)

NUEVAS TECNOLOGÍAS, PROTECCIÓN DE DATOS PERSONALES Y EL SEGURO*

NEW TECHNOLOGIES, PERSONAL DATA PROTECTION AND INSURANCE

Hoy lo más valioso del mundo
no es el oro ni el petróleo, son los datos!

*HENRIQUE JOSÉ SARAIVA LIMA***

Fecha de recepción: 13 de octubre de 2022
Fecha de aceptación: 30 de octubre de 2022
Disponible en línea: 30 de diciembre de 2022

Para citar este artículo/To cite this article

Saraiva Lima, Henrique José. *Nuevas tecnologias, protección de datos personales y el seguro,* 57 Rev.Ibero-Latinoam.Seguros, 249-270 (2022). https://doi.org/10.11144/Javeriana.ris57.ntps

doi:10.11144/Javeriana.ris57.ntps

* Ponencia presentada en el XVII Congreso Iberolatinoamericano de Seguros CILA-AIDAen Agosto de 2022 en San José, Costa Rica.

** Licenciado en Derecho por la Universidad Católica de Lisboa (Portugal) en Julio de 1982. Abogado especializado en el área de derecho internacional del transporte, derecho de seguros y derecho internacional. Socio principal del Bufete de Abogados "Saraiva Lima e Associados" fundado en abril de 1995, con oficinas en Lisboa y Oporto. Consultor Senior en Derecho de Transporte colaborando para Naciones Unidas (UNCTAD), con misiones en Mozambique (1994), Angola (1995 y 1996) y Palestina (2013). Contacto: saraivalima@saraivalima.com.

RESUMEN

El Reglamento (UE) 2016/79 vino a establecer, a nivel de la Unión Europea, las reglas relativas a la protección de las personas en lo que dice respecto al tratamiento de datos personales y a la libre circulación de esos datos y prevé un conjunto amplio de principios y normas que tiene como finalidad ultima la defensa de la privacidad de las personas y permite que los ciudadanos europeos controlen mejor sus datos personales.

El tratamiento de los datos personales es lícito si el titular de los datos hubiera dado su consentimiento para una o más finalidades específicas, lo cual debe ser libremente prestado, específico, informado y expreso.

En lo que respecta a la actividad aseguradora el tratamiento de los datos personales es manifiestamente indispensable pues no es posible celebrar un contrato de seguro sin que el asegurado provea a la aseguradora los datos personales considerados necesarios a la aceptación de la propuesta de seguro.

Esta problemática es particularmente importante en el sector asegurador una vez que son cada vez más frecuentes los casos de utilización de las páginas web y de los servicios digitales de las aseguradoras, a través de los cuales los utilizadores pueden recoger informaciones sobre los seguros comercializados por la aseguradora, efectuar simulaciones a fin de conocer el valor de la prima de un determinado seguro y presentar propuestas de seguro con vista a la emisión de una póliza de seguro.

La transmisión de datos personales por parte del asegurado y el tratamiento de los mismos por parte de la aseguradora obedece al principio de limitación de las finalidades según el cual los datos personales deben ser recogidos para fines determinados, explícitos y legítimos no pudiendo ser tratados para otros fines que no los previstos.

El tema de la protección de datos personales asume particular relevancia cuando están en causa seguros de personas, como es el caso de seguro de salud y del seguro de vida con cobertura de los daños por muerte e invalidez.

La cuestión de la seguridad asume una importancia capital cuando hablamos en protección de datos personales y, en especial, cuando están en causa datos sensibles que tienen que ser tratados en el ámbito de la fase pre contractual y durante la vigencia de los seguros de personas.

Los riesgos cibernéticos están en permanente evolución, afectan a todos y son cada vez más frecuentes y agresivos los ataques cibernéticos por lo que podemos afirmar que hoy nadie (personas, empresas, organizaciones y Gobiernos) están inmunes o está a salvo de ataques cibernéticos.

Palabras Clave: Reglamento (UE) 2016/79, Protección de datos personales, seguros de personas, riesgos cibernéticos.

ABSTRACT

At the level of the European Union, Regulation (EU) 2016/79 established rules related to the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and lays out an extensive set of principles and norms which final purpose is the defense of the privacy of people and permits European citizens to control their personal data in a better fashion.

Processing of personal data is licit as long as the owner of the data had expressed her consent for one or more purposes. Such consent must be free, specific, informed and expressed.

As to the insurance activity, processing of personal data is clearly needed because it is not possible to subscribe an insurance policy without the insured entity providing the insurer with the personal data which are deemed needed in the context of accepting the insurance policy.

This problem is particularly important in the insurance sector as the number of cases of usage of webpages and digital services by means of which users can collect information about insurance policies offered by the insurance company, carry out simulations in order to know the amount of the premium of a certain insurance policy and submit proposals in order to issue an insurance policy, is growing.

Transmitting personal data on the part of the insured party and the processing thereof by the insurance company responds to the principle of limitation of purposes according to which personal data must be collected for specific, explicit and legitimate purposes and data cannot be processed for purposes other than the ones expressly set out.

The issue of processing of data is particularly important in the case of persons insurance policies and in particular when sensible data must be processed in the precontractual stage and throughout the term of personal insurance policies.

Cybernetic risks are constantly evolving, affect all and cybernetic attacks are growingly frequent and aggressive; therefore, it can be stated that today nobody (companies, organizations, governments) is immune to cybernetic attacks.

Keywords*: Regulation (EU) 2016/79, personal data protection, personal insurance, cybernetic risks.*

SUMARIO

1. INTRODUCCIÓN AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El Reglamento (UE) 2019/79 del Parlamento Europeo y del Consejo de 27 de abril de 2016 establece, a nivel de la Unión Europea, las reglas relativas a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

Son defendidos los derechos y libertades fundamentales de los ciudadanos europeos y, en especial, su derecho a la protección de los datos personales.

Este Reglamento General de Protección de Datos, en adelante designado por RGPD, entró en vigor, de forma simultánea, el día 25 de mayo de 2018 en todos los Estados-Miembros de la Unión Europea.

Por el hecho de tratarse de un Reglamento, no hubo necesidad de transposición en cada uno de los Estados- Miembros.

No obstante, el Estado Portugués optó por aprobar y publicar la Ley nº 58/2019 que asegura la ejecución del referido Reglamento en el ordenamiento jurídico nacional.

Este Reglamento se encuadra en una perspectiva más amplia que se asienta en la defensa del derecho a la privacidad y en la tutela de la vida privada.

Esta esencialmente en causa la salvaguardia de la información personal, incluyendo la que tiene carácter íntimo, reservado y confidencial.

En ese contexto, el RGPD prevé un conjunto amplio de principios y normas que tiene como finalidad última la defensa de la privacidad de las personas.

El RGPD permite que los ciudadanos europeos controlen mejor sus datos personales.

En realidad, están previstas medidas que permiten el acceso facilitado de los ciudadanos a sus propios datos y fue creado un nuevo derecho a la portabilidad de los datos que facilita la transmisión de datos personales entre entidades diferentes.

En esta intervención vamos a hablar sobre el contrato de seguro y la utilización de la información referente a datos personales disponible, recogida y utilizada en el ámbito de la actividad aseguradora.

El tema asume particular relevancia cuando están en causa seguros de personas, como es el caso de los seguros de salud y de los seguros de vida con cobertura de los daños por muerte e invalidez.

Se trata de un tema actual que preocupa al sector de los seguros dado que, sin tratamiento de datos personales, no es posible celebrar un contrato de seguro.

2. ÁMBITO DE APLICACIÓN DEL RGPD

El RGPD se aplica al tratamiento de datos personales por medios total o parcialmente automatizados, bien como el tratamiento por medio no automatizados de datos personales contenidos en ficheros o a ellos destinados.

Los titulares de los datos personales son personas físicas, ciudadanos europeos, que, tras la publicación del RGPD, se benefician de un conjunto amplio de derechos.

Tales datos son transmitidos para una cierta y determinada finalidad, à las entidades, designadas por responsables por el tratamiento de los mismos que, por fuerza del RGPD están vinculadas a un sin número de obligaciones.

A nivel territorial, el RGPD se aplica al tratamiento de datos personales efectuado por empresas con sede en la Unión Europea bien como por empresas no europeas que ofrecen servicios o realizan negocios en Europa.

Cuando el tratamiento de datos personales fuera efectuado por un responsable no establecido en el territorio de la Unión Europea, el RGPD es aplicable si las actividades de tratamiento estuvieran relacionadas con:

a) la oferta de bienes y servicios de esos titulares de datos personales en la Unión Europea;

b) el control de su comportamiento, desde que ese control tenga lugar en la Unión Europea.

La cuestión del control de comportamiento de los ciudadanos en el interior de la Unión Europea ha generado controversias, una vez que está en causa saber si una determinada actividad de tratamiento puede (o no) ser considerada control de comportamiento de titulares de datos.

Este tema del control del comportamiento se habló mucho en el Reino Unido en relación con la campaña Brexit.

Para el efecto, es relevante saber si las personas son seguidas en internet bien como la potencial utilización posterior de técnicas de tratamiento de datos especiales con vista a definir el perfil de una determinada persona bien como sus preferencias, o su comportamiento y sus aptitudes.

3. PRINCIPIOS APLICABLES

El RGPD se asienta en seis principios fundamentales:

a) el principio de licitud, lealtad y transparencia:

Este principio prevé que los datos personales sean objeto de un tratamiento lícito, leal y transparente en relación al respectivo titular.

b) el principio de la limitación de las finalidades:

De acuerdo con este principio, los datos personales deben ser recogidos para fines determinados, explícitos y legítimos, no pudiendo ser tratados para otros fines que no los previstos.

c) el principio de minimización de los datos:

Transcurre de este principio que los datos deben ser limitados a lo que es necesario relativamente a las finalidades para las cuales son tratados.

d) el principio de exactitud;

Este principio presupone que los datos sean exactos y que sean actualizados siempre que sea necesario.

e) el principio de la limitación de conservación:

Este principio establece que los datos deber ser conservados apenas y durante el periodo estrictamente necesario para las finalidades con que fueron recogidos y tratados.

f) el principio de la integridad y confidencialidad:

Finalmente, este principio obliga a que estuviera garantizada la seguridad de los datos, de modo a que no sean utilizados de forma ilícita y que no sean destruidos.

4. EL CONSENTIMIENTO DEL TITULAR DE LOS DATOS

El tratamiento de los datos personales es licito si el titular de los datos hubiera dado su consentimiento para una o más finalidades específicas.

El titular de los datos asume un papel absolutamente fundamental en el contexto de la protección de datos y, como no podía dejar de ser, en el sistema establecido por el RGPD.

El consentimiento del titular de los datos debe ser:

a) libremente prestado, o sea, sin cualquier condiciones o exigencias;

b) específico, destinado a una finalidad u operación determinada;

c) informado, exigiendo que al titular le sean transmitidas todas las aclaraciones necesarias y relevantes para comprender lo que está autorizando;

d) expreso, debiendo constar de una declaración clara e inequívoca a través de la cual el titular de los datos manifiesta su concordancia.

La lógica del sistema impone que las personas, en cuanto titulares de datos personales, puedan confiar en las entidades a quien esos datos son transmitidos para las finalidades ciertas y determinadas y seguramente legítimas que justifican ese tratamiento.

El responsable por el tratamiento de los datos personales debe estar en condiciones de, en cualquier momento y siempre que fuera necesario, demostrar que el titular de esos datos dio su consentimiento.

La licitud del consentimiento es medida en función de la finalidad tal como fue definida por el responsable por el tratamiento de los datos personales y debe incluir, apenas y solamente, la información estrictamente necesaria.

El consentimiento tiene que ser expreso e inequívoco pero el titular de los datos puede, en cualquier momento, retirar ese consentimiento.

5. TIPOS DE TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales es definido en el RGPD como una operación o un conjunto de operaciones efectuadas sobre datos personales o sobre conjuntos de datos personales, por medios automatizados o no automatizados.

El tratamiento de datos personales integra un amplio conjunto de actividades u operaciones, a saber:

a) la recogida;

b) el registro;

c) la organización;

d) la estructura;

e) la conservación,

f) la adaptación o alteración;

g) la recuperación;

h) la consulta;

i) la utilización;

j) la divulgación por transmisión;

k) la difusión o cualquier otra forma de disponibilidad;

l) la comparación o interconexión;

m) la limitación;

n) y la eliminación o destrucción;

A todas y a cada una de estas actividades u operaciones se aplican los principios y reglas previstos en el RGPD.

El RGPD prohíbe, en regla, el tratamiento de datos personales que revelen el origen racial o étnica, las opiniones políticas, las convicciones religiosas o la filiación sindical del titular.

También está prohibido el tratamiento de datos relativos a la vida sexual u orientación sexual de las personas.

6. EL RESPONSABLE POR EL TRATAMIENTO DE LOS DATOS PERSONALES

El responsable por el tratamiento de los datos personales está obligado a asegurar y comprobar que ese tratamiento es realizado de acuerdo con las normas y principios previstos en el RGPD.

Se prevé la existencia de un código de conducta y de procedimientos de certificación que fueron aprobados son esenciales para el responsable poder demostrar que da cumplimiento a sus obligaciones legales.

Deben ser aplicadas las medidas técnicas y organizativas necesarias para asegurar un nivel de seguridad adecuada al riesgo de forma a evitar violaciones de datos personales, con todas las consecuencias derivadas para el respectivo titular.

Los titulares de datos personales que hayan sufrido daños patrimoniales y no patrimoniales en consecuencia de una violación del RGPD, entre otros a nivel del acceso ilícito o ilegitimo a sus datos por parte de terceros, pueden solicitar el pago de una indemnización al responsable.

El responsable por el tratamiento de datos personales asume igualmente las responsabilidades resultantes de la intervención de los subcontratantes que fueran contratados para el efecto.

Se entiende por subcontratante, cualquier persona física o jurídica, que trate los datos personales a pedido y por cuenta del responsable.

El sistema de protección de datos personales se basa en el responsable del tratamiento de estos datos.

Hoy en día se habla mucho de inteligencia artificial y es posible que se pueda utilizar un sistema de inteligencia artificial en el proceso de procesamiento de datos.

En este caso, el responsable del tratamiento de los datos personales asume toda la responsabilidad derivada del uso de la inteligencia artificial.

La máquina no es responsable; la responsabilidad siempre recae en un individuo.

Lo mismo ocurre cuando el RGPD habla de subcontratistas y de la responsabilidad por la intervención de estos subcontratistas.

7. EL DERECHO AL OLVIDO

El titular de los datos tiene el derecho a la eliminación de los datos que se consubstancia en el derecho a obtener del responsable por el tratamiento la garantía de que sus datos serán eliminados.

El ejercicio de ese derecho presupone que haya ocurrido una de las siguientes situaciones:

a) los datos dejaron de ser necesarios para la finalidad con que fueron transmitidos;

b) el titular de los datos retiró su consentimiento;

c) el titular de los datos se opone al tratamiento y no existen intereses legítimos prevalecientes;

d) el titular de los datos se opone al tratamiento para efectos de marketing directo;

e) los datos personales fueron utilizados de forma ilícita;

f) los datos personales tienen que ser apagados para el cumplimiento de una obligación legal a que el responsable por el tratamiento esté vinculado;

g) los datos personales que se refieran a un menor de 16 años y fueran recogidos en el contexto de la oferta de servicios de la sociedad de información.

El responsable debe, después de solicitado por el titular de los datos, apagar sin demora los datos que hayan sido transmitidos.

Existen algunos casos en que el derecho al olvido no es aplicable.

Son los casos, entre otros, en que existe un interés público, un motivo de salud pública, el cumplimiento de una obligación legal o para efectos de ejercicio o defensa en un proceso judicial.

La posición de las aseguradoras en relación con el derecho al olvido es complicada.

Por un lado, están obligados a suprimir los datos personales cuando ya no sean necesarios para la finalidad para la que fueron transmitidos.

Esto es lo que sucede cuando el contrato de seguro llega a su fin.

Pero, por otro lado, tienen derecho a conservar sus datos personales para el ejercicio o la defensa en un procedimiento judicial.

Si la disputa legal es previsible o inminente, la cuestión no se plantea puesto que prevalece el derecho a mantener los daños y perjuicios para el ejercicio o defensa en el proceso que se entablará contra el asegurador.

El problema surge cuando se trata de litigios que no eran previsibles, constituyendo una auténtica sorpresa para la aseguradora.

En Portugal, en materia de responsabilidad civil extracontractual, el derecho a la indemnización caduca en un plazo de tres años a partir de la fecha en que el perjudicado tuvo conocimiento del derecho que le corresponde.

Si el acto ilícito constituye un delito, el plazo puede ser mayor, según el tipo de delito de que se trate.

En caso de litigio entre el asegurado y el asegurador, el plazo de prescripción aplicable es de cinco años a partir de la fecha en que el asegurado tuvo conocimiento del derecho.

Con plazos tan largos, puede ocurrir que, cuando el asegurador sea citado para impugnar determinada acción judicial que no estaba prevista, ya no tenga en su poder datos personales que eran imprescindibles para su defensa.

8. AUTORIDADES DE CONTROL

El RGPD prevé la existencia de autoridades nacionales de control creadas por los Estados-Miembros a quien cabe la fiscalización de la aplicación de las normas previstas en el Reglamento.

Esas autoridades ejercen sus funciones con total independencia en la prosecución de sus atribuciones.

Las autoridades de control disponen de poderes de investigación, poderes de corrección, poderes consultivos y poderes de autorización.

9. EL DEBER DE INFORMACIÓN

En lo que respecta a la actividad aseguradora el tratamiento de datos personales es manifiestamente indispensable a la celebración del contrato de seguro.

No es posible celebrar un contrato de seguro sin que el tomador del seguro / asegurado entregué a la aseguradora los datos personales considerados necesarios e indispensables a la aceptación de la propuesta de seguro.

En Portugal está en vigor desde el día 1 de enero de 2009 el Régimen Jurídico del Contrato de Seguro que fue aprobado por el Decreto-Ley N° 72/2008.

En este régimen legal fue dada particular relevancia a la defensa de la posición del asegurado –en cuanto parte contractual más débil en esta relación jurídica– pero también fue definido un conjunto de deberes pre contractuales a que estos están obligados, ente otros al nivel de la información a la aseguradora.

Está previsto el principio según el cual la declaración inicial del riesgo es de la responsabilidad del asegurado.

El asegurado está obligado, antes de la celebración del contrato, a declarar con exactitud todas las circunstancias que conozca y razonablemente deba tener por significativas para la apreciación del riesgo por la aseguradora.

Este principio es aplicable mismo en relación a información cuya mención no conste del cuestionario pre elaborado por la aseguradora.

Esta, sin embargo, la aseguradora obligada, antes de la contratación del seguro, a aclarar al asegurado acerca de este deber y a alertarlo para las consecuencias derivadas de su incumplimiento.

El objetivo subyacente a este deber es el de asegurar que el asegurado tiene noción de la relevancia de las declaraciones e informaciones constantes de la propuesta de seguro que irán a servir de base a la apreciación del riesgo por parte de la aseguradora con la consecuente aceptación (o no) del seguro.

El asegurado no puede, más tarde y en caso de siniestro, venir a decir que no sabía que estaba obligado al cumplimiento de los deberes de información que están previstos en la ley, prestando todas las informaciones relevantes para la celebración del contrato de seguro.

En Portugal se acostumbra a decir que el desconocimiento de la ley no exime de su cumplimiento.

Esta frase traduce lo dispuesto en el artículo 6º de nuestro Código Civil que establece que "El desconocimiento o la mala interpretación de la ley no justifica la falta de su cumplimiento ni exime a las personas de las sanciones en ella establecidas".

Se verifica, sin embargo, que el incumplimiento del deber de información por parte del asegurado, por regla, sólo es verificado después de la ocurrencia del siniestro.

Está en causa el principio de exactitud previsto en el RGPD que presupone que los datos personales transmitidos por el asegurado sean exactos y verdaderos.

Podrá ser planteada la cuestión de saber si la omisión de las informaciones es dolosa o meramente negligente.

El incumplimiento doloso del deber de información por parte del asegurado confiere a la aseguradora el derecho de anular el contrato de seguro con efectos retroactivos y no devolver el valor de las primas que recibió.

Los Tribunales Portugueses consideran que no es necesaria la existencia de un nexo de causalidad entre los hechos omitidos y el siniestro cubierto por el seguro.

En el caso de haber sido probado que la omisión del deber de información es meramente negligente, la aseguradora tiene el derecho de resolver el contrato.

Debe demostrar que, en ningún caso, habría celebrado el contrato si hubiese conocido el hecho omitido o declarado inexactamente, y, si fuera ese el caso, no está obligada a cubrir el siniestro y pagar la indemnización correspondiente, pero tendrá que devolver el valor de las primas de seguro.

Cuando hablamos de deber de información a que está obligado el asegurado en el momento de la contratación del seguro, están esencialmente en causa datos personales que tienen que ser transmitidos a la aseguradora de forma a que ésta, después de analizar el riesgo, puede aceptar (o no) la propuesta de seguro.

El cumplimiento del deber de información a que está vinculado el asegurado también existe cuando, durante la vigencia del contrato, se verifique alguna situación de modificación del riesgo.

Así, el asegurado está obligado a comunicar a la aseguradora, durante la vigencia del contrato todos los hechos que provocan una modificación del riesgo inicial.

Si el asegurado no entrega la propuesta de seguro todo un conjunto de datos que le dicen respecto y que son relevantes para el análisis del riesgo, no será posible la aseguradora avanzar en el sentido de la aceptación de esa propuesta y emisión de la respectiva póliza.

Aquí se trata de la buena fe precontractual.

Conforme ya dije, no es posible celebrar un contrato de seguro sin que el asegurado entregué a la aseguradora los datos personales considerados necesarios e indispensables a la aceptación de la propuesta de seguro.

La transmisión de datos personales por parte del asegurado y el tratamiento de los mismos por parte de la aseguradora obedece al principio de la limitación de las finalidades según el cual los datos personales deben ser recogidos para fines determinados, explícitos y legítimos no pudiendo ser tratados para otros fines que no los previstos.

Es importante también tener en consideración el principio de minimización de los datos del cual deriva que los datos deben ser limitados al que es necesario relativamente a las finalidades para las cuales son tratados.

10. SEGUROS DE PERSONAS

El tema de protección de datos personales asume particular relevancia cuando están en causa seguros de personas, como es el caso del seguro de salud y del seguro de vida con cobertura de los daños por muerte e invalidez.

El contrato de seguro se asiente en la imprevisibilidad y en la incerteza a los riesgos cubiertos.

Los seguros de las personas son, en general, seguros de larga duración que se renuevan todos los años.

En este tipo de seguros, existe un cuestionario clínico que forma parte integrante de la propuesta de seguro suscrita por el asegurado.

La aceptación (o no) de la propuesta de seguro por parte de la aseguradora depende de las respuestas dadas por el asegurado a ese cuestionario clínico.

Los datos relativos a salud están definidos en el RGPD como los datos personales relacionados con la salud física o mental de una persona que revelen informaciones sobre su estado de salud.

Los cuestionarios incluyen preguntas sobre los dados biométricos del asegurado.

Estos datos corresponden a datos personales resultantes de un tratamiento técnico relativo a las características físicas, fisiológicas y comportamentales de una persona que permitan o confirmen su identidad.

Pueden también ser incluidas preguntas sobre los datos genéticos del asegurado.

Aquí, están en causa datos personales relativos a las características genéticas, hereditarias o adquiridas de una persona que proveen informaciones únicas sobre la fisiología o la salud de esa persona y que pueden resultar de un análisis de una muestra biológica.

Los cuestionarios incluyen también un sin número de preguntas, entre otras a nivel del cumplimiento de obligaciones profesionales, del rechazo del seguro por parte de otra aseguradora, de la realización regular de viajes al extranjero, de la atribución de eventuales desvalorizaciones por incapacidad física o funcional, de la realización de

tratamientos de desintoxicación (alcoholismo o toxico-dependencia), de la toma de medicamentos, del uso de gafas, de la realización de exámenes de diagnóstico, de la sumisión a intervenciones quirúrgicas y de la existencia (o no) de un grande número de enfermedades o de cualquier otras que no estén específicamente indicadas en el cuestionario.

Más recientemente, las aseguradoras añadirán al cuestionario clínico preguntas sobre el COVID-19 y, en el caso de la enfermedad haber sido ya diagnosticada, sobre las eventuales secuelas inmediatas y secuenciales resultantes de ese virus.

Estamos, como es obvio, a hablar de datos personales sensibles por cuanto son informaciones confidenciales o reservadas relativas a la condición física o mental del asegurado, hábitos personales, antecedentes médicos y hospitalarios, etc.

Se comprende que, en función de las finalidades que están en causa, la aseguradora tendrá el derecho de solicitar al asegurado informaciones de esta naturaleza, pero la sensibilidad de las mismas obliga a un rigor mayor por parte de quien va a tratar esos datos personales.

En ese sentido, las aseguradoras incluyen en su propuesta de seguro una declaración de protección de datos personales que tiene que ser firmada por el asegurado.

Es mencionado en esa declaración que las omisiones, inexactitudes y falsedades, referentes o relacionadas con la información necesaria para el tratamiento de datos efectuado en el ámbito del seguro son de la responsabilidad del asegurado.

El asegurado tiene que dar su consentimiento expreso para el tratamiento de los datos personales y sensibles.

Este consentimiento representa y confirma la causa de la licitud del tratamiento de datos personales sin el cual no sería posible aceptar y formalizar la cobertura de riesgos propuestos.

Está, igualmente, prevista la autorización expresa de la aseguradora a proceder a la recogida de otros datos personales junto de entidades terceras desde que sean necesarios a la gestión el contrato de seguro.

11. SINIESTROS

El tratamiento de los datos personales es indispensable en la fase de la contratación del seguro pero también es esencial después de la participación de un siniestro.

Conforme referí, los problemas relativos a la protección de datos personales asumen particular relevancia cuando están en causa seguros de personas, como es el caso de seguro de salud y de seguro de vida con cobertura de los daños por muerte e invalidez.

Los datos de salud a transmitir por el asegurado son esenciales para la aseguradora proceder al análisis del riesgo y aceptar (o no) el seguro que le es propuesto.

Pero tales datos también parecen esenciales en caso de siniestro.

Está previsto en la ley portuguesa que en la participación del siniestro el asegurado debe explicar las circunstancias en que ocurrió el siniestro, las eventuales causas del mismo y las respectivas consecuencias.

El asegurado está, así, obligado a prestar a la aseguradora todas las informaciones sobre el siniestro y ésta tiene derecho a desarrollar todas las diligencias que considere necesarias para la averiguación de los hechos.

En las propuestas de seguro de personas, hay declaraciones en sentido de autorizar la aseguradora, en caso de siniestro, a solicitar a los hospitales, a los médicos, a la seguridad social y a otras entidades, los datos clínicos referentes al origen, causas y evolución de la enfermedad o del accidente.

El consentimiento prestado por el asegurado (titular de los datos) abarca también el eventual intercambio de los datos con entidades terceras, como es el caso de los peritos, a quien la aseguradora recurre en caso de siniestro.

Conforme ya referí, por regla la aseguradora sólo tiene conocimiento del incumplimiento del deber de información por parte del asegurado después de la ocurrencia del siniestro.

El objetivo de la aseguradora es muy claro y consiste en conocer todas las circunstancias en que ocurrió el siniestro, de forma a poder concluir si el mismo puede ser encuadrado en el ámbito de cobertura de la póliza o si, por el contrario, hay lugar a la aplicación de alguna cláusula de exclusión.

12. LA POLÍTICA DE USO DE COOKIES

Cookies son pequeños ficheros con información relevante que son almacenados en los ordenadores por los *browsers*.

Son datos enviados a los utilizadores cuando visitan una página de internet siendo que la mayoría de los programas de navegación en internet está definida para aceptar cookies.

Los cookies son consideradas herramientas esenciales de la navegación online una vez que permiten una navegación más rápida y eficiente.

Sirven, también, para ayudar el gestor de una determinada página a averiguar la utilidad, el interés y el número de utilizadores o visitantes de esa página.

Existen dos categorías de cookies: los permanentes y los de sesión.

Los cookies permanentes quedan almacenados a nivel del browser en el disco duro del ordenador del utilizador hasta que expiren o sean excluidos.

Son utilizados siempre que es hecha una nueva visita a la página web y sirven para direccionar la navegación de acuerdo con los intereses o necesidades del utilizador.

Los cookies de sesión son temporales y, como su nombre indica, permanecen en el archivo del browser hasta terminar la visita, siendo inmediatamente eliminados.

La información obtenida por esos cookies permite al gestor de la página web analizar los patrones de tráfico y proveer una mejor experiencia de navegación.

Se verifica un aumento gradual de cookies que son usados para acompañar la actividad online de los utilizadores a lo largo del tiempo.

El objetivo es conocer los hábitos de navegación de los utilizadores de forma a ser definidos los respectivos perfiles a fin de poder posteriormente ser vendidos a una empresa de marketing para ciertos y determinados fines publicitarios o sean utilizados de forma ilícita o ilegal.

En cuanto a tipos de cookies, podemos distinguir los siguientes: cookies estrictamente necesarios, cookies analíticos, cookies de funcionalidad, cookies de publicidad y cookies de terceros.

Los cookies estrictamente necesarios permiten la navegación en la página web para acceder a áreas seguras y, sin ellos, los servicios no podrían ser presentados.

Los cookies analíticos se destinan a la recogida de información para fines estadísticos.

Los cookies de funcionalidad se destinan a guardar las preferencias de los utilizadores relativamente a la utilización de la página web, de forma a que no sea necesario volver a configurar las definiciones.

Los cookies de terceros miden el suceso de aplicación y la eficiencia de la publicidad de terceros.

Finalmente, los cookies de publicidad se destinan a direccionar la publicidad, a través de campañas de marketing, en función de los intereses de cada utilizador.

Conforme vengo refiriendo, la principal preocupación del RGPD consiste en la defensa del derecho a la privacidad y en la tutela de la vida privada.

Así siendo, importa ahora verificar lo que mudo, en materia de cookies, con la entrada en vigor del RGPD.

La principal mudanza consiste en la obligación de obtener el consentimiento por parte del utilizador.

Ese consentimiento, que debe ser expreso e informado, depende del tipo de cookies que está en causa.

Los utilizadores de las páginas web tienen el derecho de, en cualquier momento, optar por aceptar o rechazar los cookies debiendo la web presentar un aviso muy claro con esa opción, de forma a poder ser obtenido el consentimiento expreso de los utilizadores.

Los utilizadores tienen, en todo el tiempo, la posibilidad de configurar su browser para aceptar o rechazar todos y cualesquier cookies.

Esta problemática es particularmente importante en el sector asegurador una vez que son cada vez más frecuentes los casos de utilización de las páginas web y de los servicios digitales de las aseguradoras, que, en su conjunto, integran el concepto de plataformas.

A través de esas plataformas, los utilizadores pueden recoger informaciones sobre los seguros comercializados por la aseguradora, efectuar simulaciones a fin de conocer el valor de la prima de un determinado seguro y presentar propuestas de seguro con vista a la emisión de una póliza de seguro.

Quien efectúa una simulación a través de la plataforma de una aseguradora tiene necesariamente de proveer algunos datos personales teniendo como finalidad la creación de un perfil, elemento esencial para que la aseguradora pueda evaluar el riesgo a cubrir.

13. LA CUESTIÓN DE LA SEGURIDAD

La cuestión de la seguridad asume una importancia capital cuando hablamos en protección de datos personales y, en especial, cuando están en causa datos sensibles que tienen que ser tratados bien en el ámbito de la fase pre contractual bien durante la vigencia de los seguros de personas.

Las nuevas tecnologías y, en especial la internet, entraron definitivamente en las vidas de las personas y de las empresas y hoy no conseguiríamos vivir sin ellas.

También es absolutamente verdad que hoy nadie (personas, empresas organizaciones y Gobiernos) es inmune o está a salvo de ataques cibernéticos.

Dependemos de las nuevas tecnologías, pero vivimos en un mundo inseguro en lo que dice respecto a los riesgos cibernéticos.

Los riesgos cibernéticos están en permanente evolución, afectan a todos y son cada vez más frecuentes y agresivos los ataques cibernéticos.

La guerra de Ucrania vino a aumentar los riesgos cibernéticos y existen innumerables casos, algunos conocidos y otros que, por razones de seguridad, quedan en "secreto de los Dioses", de ataques cibernéticos contra entidades públicas, organizaciones, empresas privadas y personas.

Conforme referí al inicio de esta intervención "Hoy lo más valioso del mundo no es el oro ni el petróleo, son los datos".

Uno de los principios enunciados en el RGPD es el principio de la integridad y confidencialidad.

De acuerdo con este principio los datos personales deber ser tratados de una forma que garantice su seguridad, incluyendo la protección contra su tratamiento no autorizado o ilícito y contra su perdida, destrucción o damnificación accidental.

Las aseguradoras tienen la obligación de adoptar una adecuada política de protección de datos a través de la implementación de medidas de seguridad destinadas a evitar la divulgación indebida, accidental o intencional de datos personales de sus asegurados.

Las medidas de protección deben asegurar la confidencialidad de los datos personales de los asegurados y, en especial, de los datos considerados sensibles, como es el caso de los datos relativos a la salud.

Los riesgos aumentan en función de la mayor o menor confidencialidad de los datos personales de los asegurados.

Estamos en el dominio de ciberdelincuencia y muchos delitos son practicados con objetivo de obtención de importantes ventajas financieras.

El autor del delito, que raramente es identificado y localizado, pudiendo estar a millares de kilómetros de distancia, pretende, a través del chantaje, recibir dinero de la aseguradora bajo pena de divulgar, a través de internet, los datos personales de los asegurados.

La no cedencia al chantaje con la consecuente divulgación pública de los datos personales de los asegurados, podrá traducirse en daños reputacionales graves y pedidos de indemnización elevados, con todos los riesgos de ahí derivados a nivel de la situación financiera de la aseguradora.

En verdad, las aseguradoras luchan contra un enemigo invisible que no puede ser responsabilizado por los daños causados.

La presentación de una denuncia no pasa de una mera formalidad burocrática y sin ningún efecto útil.

Y no es difícil percibir que, muchas veces, la ocurrencia de un ataque cibernético no es siquiera divulgada ni llega a conocimiento de la opinión pública.

El RGPD vino a exigir una atención especial por parte de quien lidia con datos personales obligando a la implementación de reglas de seguridad de la información.

El responsable por el tratamiento de los datos está obligado a aplicar las medidas técnicas y organizativas adecuadas y necesarias para asegurar el nivel de seguridad adecuada al riego y salvaguardar la confidencialidad, la integridad, la disponibilidad y la autenticidad de la información.

Está prevista, para el efecto, la seudonimización y la cifra de los datos personales.

Se considera seudonimización el tratamiento de datos personales de forma a que dejen de poder ser directa e inmediatamente ligados a un titular de datos específico sin recurrir a informaciones complementarias.

Los campos de identificación de las personas son sustituidos por identificadores artificiales de forma a asegurar que los datos personales en causa no puedan ser atribuidos a una cierta y determinada persona.

Se trata de una doble medida de seguridad favorable a la privacidad una vez que esas informaciones complementarias deben ser mantenidas separadamente.

La cifra de los datos personales se verifica cuando los datos son codificados de tal forma que apenas pueden ser leídos y tratados por los responsables por ese tratamiento o por las personas autorizadas para tal.

La experiencia nos muestra que muchos de los riesgos de ataques informáticos son de responsabilidad de los propios utilizadores.

Debe ser definida por cada aseguradora una política de seguridad con procedimientos operacionales de seguridad a que están obligados los funcionarios autorizados a proceder al tratamiento de datos personales de los asegurados.

De esos procedimientos deben hacer parte reglas muy simples a observar por los funcionarios como sean las de bloquear siempre el ordenador cuando no lo estén utilizando, no tirar fotografías cuando hay datos sensibles en la pantalla, no guardar datos personales en el disco local del ordenador, guardar los dossiers con datos personales en armarios o cajones fechados con llave y no transmitir por el teléfono ninguna información relativa a datos personales.

También están previstas medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y de los servicios de tratamiento.

En caso de incidente, deberá estar asegurada la capacidad para restablecer la disponibilidad y el acceso a los datos personales de forma oportuna.

Finalmente, deberá ser creado por el responsable un proceso para testar, apreciar y valorar regularmente la eficacia de las medidas técnicas y organizativas destinadas a garantizar la seguridad de los datos personales.

En caso de violación de los datos personales, el responsable por el tratamiento de esos datos debe, sin demora justificativa, notificar a la autoridad de control nacional.

En esa notificación, deberá el responsable describir la naturaleza de la violación, las consecuencias probables de esa violación y las medidas adoptadas o propuestas para reparar la violación y atenuar sus efectos.

La violación de los datos personales también tendrá que ser comunicada al titular de esos datos.

14. MULTAS

La legislación portuguesa que fue publicada después de la entrada en vigor del RGPD, prevé la aplicación de multas en caso de violación de las normas previstas en el RGPD.

Las faltas graves son punidas con multas:

a) de € 2.500 a € 10.000.000 o de 2% del volumen de negocios anual, conforme la que fuera más elevada, tratándose de una grande empresa;

b) de € 1.000 a € 1.000.000 o de 2% de volumen de negocios anual, conforme la que fuera más elevada, tratándose de una pequeña o mediana empresa;

c) de € 500 a € 250.000 en el caso de personas físicas.

Las faltas muy graves son punidas con multas:

a) de € 5.000 a € 20.000.000 o de 2% de volumen de negocios anual, conforme la que fuera más elevada, tratándose de una grande empresa;

b) de € 2.000 a 2.000.000 o de 2% de volumen de negocios anual, conforme la que fuera más elevada, tratándose de una pequeña o mediana empresa;

c) de € 1.000 a € 500.000 en el caso de personas físicas.

En la determinación de la medida de la multa son tenidos en consideración, entre otros, la naturaleza, gravedad y la duración de la infracción teniendo en cuenta la naturaleza, el ámbito o el objetivo del tratamiento de datos en causa, bien como el número de titulares de datos afectado y el nivel de daños por ellos sufridos, el carácter intencional o negligente de la infracción y el grado de responsabilidad del responsable por el tratamiento ante las medidas técnicas u organizativas por el implementadas.

La violación de las reglas de seguridad constituye una falta grave.

15. CONCLUSIONES

1. El Reglamento (UE) 2016/79 del Parlamento Europeo y del Consejo de 27 de Abril de 2016 vino a establecer, a nivel de la Unión Europea, las reglas relativas a la protección de las personas en lo que dice respecto al tratamiento de datos personales y a la libre circulación de esos datos.

2. El RGPD prevé un conjunto amplio de principios y normas que tiene como finalidad ultima la defensa de la privacidad de las personas y permite que los ciudadanos europeos controlen mejor sus datos personales.

3. El RGPD se aplica al tratamiento de datos personales por medios total o parcialmente automatizados, bien como al tratamiento por medios no automatizados de datos personales contenidos en ficheros o a ellos destinados.

4. A nivel territorial, el RGPD se aplica al tratamiento de datos personales efectuado por empresas con sede en la Unión Europea bien como por empresas no europeas que ofrecen servicios o hacen negocios en Europa.

5. El RGPD se asienta en seis principios fundamentales: de licitud, de lealtad y transparencia, de la limitación de las finalidades, de la minimización de los datos, de la exactitud, de la limitación de la conservación y de la integridad y confidencialidad.

6. El tratamiento de los datos personales es lícito si el titular de los datos hubiera dado su consentimiento para una o más finalidades específicas, lo cual debe ser libremente prestado, específico, informado y expreso.

7. El tratamiento de datos personales integra un amplio conjunto de actividades u operaciones: la recogida, el registro, la organización, la estructuración, la conservación, la adaptación o alteración, la recuperación, la consulta, la utilización, la divulgación por transmisión, la difusión o cualquier otra forma de disponibilidad, la comparación o interconexión, la limitación y la eliminación o la destrucción.

8. El responsable por el tratamiento de los datos personales está obligado a asegurar y comprobar que ese tratamiento es realizado de acuerdo con las normas y principios previstos en el RGPD y debe aplicar las medidas técnicas y organizativas necesarias para asegurar un nivel de seguridad adecuado al riesgo de forma a evitar cualquier violación de datos personales, con todas las consecuencias de ahí derivadas para el respectivo titular.

9. El titular de los datos tiene el derecho a eliminar los datos que se consubstancia en el derecho a obtener del responsable por el tratamiento la garantía de que sus datos serán eliminados sin demora.

10. El RGPD prevé la existencia de autoridades nacionales de control creadas por los Estados-Miembros que ejercen sus funciones con total independencia y disponen de poderes de investigación, de corrección, consultivos y de autorización.

11. En lo que respecta a la actividad aseguradora el tratamiento de los datos personales es manifiestamente indispensable pues no es posible celebrar un contrato de seguro sin que el asegurado provea a la aseguradora los datos personales considerados necesarios a la aceptación de la propuesta de seguro.

12. La declaración inicial del riesgo es de responsabilidad del asegurado por lo que está obligado, antes de la celebración del contrato, a declarar con exactitud todas las circunstancias que conozca y razonablemente deba tener por significativas para la apreciación del riesgo por la aseguradora, mismo en relación a informaciones cuya mención no conste del cuestionario elaborado por la aseguradora.

13. Está en causa el principio de exactitud previsto en el RGPD que presupone que los datos personales transmitidos por el asegurado sean exactos y verdaderos.

14. La omisión de las informaciones pre contractuales por parte del asegurado puede ser dolosa o meramente negligente, confiriendo a la aseguradora, conforme el caso, el derecho a anular o a resolver el contrato de seguro.

15. La transmisión de datos personales por parte del asegurado y el tratamiento de los mismos por parte de la aseguradora obedece al principio de limitación de las finalidades según el cual los datos personales deben ser recogidos para fines determinados, explícitos y legítimos no pudiendo ser tratados para otros fines que no los previstos.

16. El tema de la protección de datos personales asume particular relevancia cuando están en causa seguros de personas, como es el caso de seguro de salud y del seguro de vida con cobertura de los daños por muerte e invalidez.

17. En este tipo de seguros, la aceptación (o no) de la propuesta de seguro por parte de la aseguradora depende de las respuestas dadas por el asegurado a ese cuestionario clínico.

18. Los datos relativos a la salud están definidos en el RGPD como los datos personales relacionados con la salud física o mental de una persona que revelen informaciones sobre su estado de salud.

19. Estamos ante datos personales sensible por tanto se trata de informaciones confidenciales o reservadas relativas a la condición física o mental del asegurado, hábitos personales, antecedentes médicos y hospitalarios, que obligan a la aseguradora a un rigor mayor por parte de quien va a trata esos datos personales.

20. El tratamiento de los datos personales es indispensable en la fase de contratación del seguro pero también es esencial después de la participación de un siniestro.

21. En caso de siniestro, el asegurado está obligado a prestar a la aseguradora todas las informaciones sobre el siniestro y está tiene el derecho de desarrollar todas las diligencias que considere necesarias para la averiguación de los hechos, de forma a poder concluir si el siniestro está (o no) incluido en el ámbito de la cobertura de la póliza.

22. Con la entrada en vigor del RGPD, la principal mudanza a nivel de la política de cookies consiste en la obligación de obtener el consentimiento expreso e informado por parte del utilizador.

23. Los utilizadores de las páginas web tienen el derecho de, en cualquier momento, optar por aceptar o recusar los cookies, debiendo la página presentar un aviso muy claro con esa opción, de forma a poder ser obtenido el consentimiento expreso de los utilizadores.

24. Esta problemática es particularmente importante en el sector asegurador una vez que son cada vez más frecuentes los casos de utilización de las páginas web y de los servicios digitales de las aseguradoras, a través de los cuales los utilizadores pueden recoger informaciones sobre los seguros comercializados por la aseguradora, efectuar simulaciones a fin de conocer el valor de la prima de un determinado seguro y presentar propuestas de seguro con vista a la emisión de una póliza de seguro.

25. La cuestión de la seguridad asume una importancia capital cuando hablamos en protección de datos personales y, en especial, cuando están en causa datos sensibles que tienen que ser tratados en el ámbito de la fase pre contractual y durante la vigencia de los seguros de personas.

26. Los riesgos cibernéticos están en permanente evolución, afectan a todos y son cada vez más frecuentes y agresivos los ataques cibernéticos por lo que podemos afirmar que hoy nadie (personas, empresas, organizaciones y Gobiernos) están inmunes o está a salvo de ataques cibernéticos.

27. De acuerdo con el principio de integridad y confidencialidad, los datos personales deben ser tratados de una forma que garantice su seguridad, incluyendo la protección contra su tratamiento no autorizado o ilícito y contra su perdida, destrucción o damnificación accidental por lo que las aseguradoras tienen la obligación de adoptar una adecuada política de protección de datos a través de la implementación de medidas de seguridad eficaces, como es el caso de la seudonimización y cifra de los datos personales.

28. La experiencia nos muestra que muchos de los riesgos de ataques informáticos son de responsabilidad de los propios utilizadores por lo que cada aseguradora debe implementar una política de seguridad con procedimientos operacionales de seguridad a seguir por los funcionarios autorizados a proceder al tratamiento de datos personales de los asegurados.

29. El responsable por el tratamiento de los datos personales tiene la obligación de crear un proceso para atestar, apreciar y valorar regularmente la eficacia de las medidas técnicas y organizativas destinadas a garantizar la seguridad de los datos personales y, en caso de violación de datos personales, debe, sin demora justificativa, notificar a autoridad de control nacional y al titular de los datos.

30. La legislación portuguesa que fue publicada después de la entrada en vigor del RGPD, prevé la aplicación de multas en caso de violación de las normas previstas en el RGPD que podrán ir de € 2.500 a € 20.000.000 para las empresas y de € 500 a € 500.000 para las personas físicas, en función de la naturaleza, gravedad y la duración de la infracción y del carácter intencional o negligente de la infracción y el grado de responsabilidad del responsable por el tratamiento de los datos personales.

16. BIBLIOGRAFÍA

O Regulamento Geral sobre a Protecção de Dados, Márcia de Magalhães, 2019.

Colectânea de Seguros, Pedro Romano Martinez, 2008.

Problemas e Soluções de Direito dos Seguros, Luis Poças, 2020.

O Contrato de Seguro, José Vasques, 1999.

Direito da Protecção de Dados, A. Barreto Menezes Cordeiro, 2020.

Comentário ao Regulamento Geral de Protecção de Dados, Alexandre Sousa Pinheiro, Cristina Pimenta Coelho, Tatiana Duarte, Carlos Jorge Gonçalves e Catarina Pina Gonçalves, 2018.