OBSERVATORIO IBEROAMERICANO
DE PROTECCIÓN DE DATOS
Iniciativa sobre privacidad, protección de datos y habeas data en Iberoamérica

# *Declaración de Santiago*

## *Hacia una unificación de criterios sobre seguridad y protección de datos en Internet*

La Declaración de Santiago, hacia una unificación de criterios sobre seguridad y protección de datos en Internet, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, presentada en la ciudad de Santiago (Chile), el 12 de septiembre de 2013, por el Pedro Huichalaf Roa, en el transcurso de la Seminario de Datos personales, organizado en la Facultad de Derecho de la Universidad de Chile, en colaboración con la ONG META.

# *Declaración de Santiago, hacia una unificación de criterios sobre seguridad y protección de datos en Internet*

*La protección de datos personales es un derecho humano universal y fundamental reconocido a nivel global en la Declaración Universal de los Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos. Íntimamente ligado con la libertad individual, la libertad de expresión y el derecho a la intimidad, honor y dignidad personal, está consagrado por el artículo 8 de la Carta Europea de Derechos Fundamentales, y regulado como garantía constitucional en la mayoría de ordenamientos jurídicos iberoamericanos en el marco del "habeas data".*

*Sin embargo, la revolución tecnológica en lo que nos hallamos inmersos como consecuencia de la aparición de Internet ha producido y está produciendo innumerables cambios en los hábitos y las relaciones humanas, que obligan a las distintas legislaciones a un ejercicio de permanente adaptación a una realidad cambiante y transfronteriza. Con el uso de las nuevas tecnologías, y en particular con la eclosión de la red y las nuevas formas de interacción de las personas, diariamente se ven afectados los derechos y libertades individuales y colectivas. Aquellos derechos referidos a derechos de propiedad sobre bienes inmateriales como los relacionados con los derechos de autor y la propiedad industrial, todos los relacionados con el comercio electrónico, como los derechos de consumidores y usuarios, o aquellos relativos a la libertad de expresión e información. Pero sin duda el derecho más amenazado y vulnerable, y sobre el que deviene fundamental articular una regulación unificada, adecuada, solvente y eficaz, es el derecho a la protección de datos personales, dentro del marco de la protección a la intimidad personal, que si bien como hemos apuntado en la introducción ya es objeto de regulación a nivel nacional, supranacional e internacional, aún carece de una regulación actualizada y unificada que garantice su tutela efectiva, debido a la realidad cambiante derivada de los constantes avances*

*tecnológicos, y a la ausencia de un marco común que supere las barreras nacionales, ya que solo así puede ser tratado un fenómeno que no entiende de fronteras.*

*Internet se ha consolidado en una herramienta de gran utilidad con múltiples usos y finalidades. La posibilidad de poder encontrar cualquier tipo de información en segundos, las utilidades para el teletrabajo, el almacenamiento de información, el ocio o las relaciones sociales son ilimitadas.* No podrá negarse que la tecnología digital, se ha convertido en eje fundamental de los grandes cambios a los que asiste esta generación nuestra, tanto en la manera de relacionamos con los demás, como en la forma de entender los negocios.

*Los productos o servicios disponibles a través de la red pueden ser remunerados o gratuitos. Ambas presentan problemas para mantener a buen recaudo la privacidad de los datos de sus usuarios y la manera en como se brinda la información relevante para que el usuario tome una decisión, elección, uso o consumo de un determinado servicio.*

*Los servicios remunerados usan los datos de sus usuarios para su propio beneficio y así poder brindar mejoras en la prestación de sus servicios ya que mantienen a su alcance datos analizados con los cuales generan perfiles de usuarios lo cual es licito siempre que se le brinde informacion relevante, oportuna, veraz, suficiente, de fácil comprensión y fácilmente accesible debiendo ser brindada en el idioma oficial del país de cada usuario.*

*Los Servicios gratuitos también están obligados a cumplir con brindar informacion relevante entendiendo esta como la información mínima sin la cual el usuario no hubiera adoptado la decisión de usar el servicio y entablar una relación de consumo a cuya ejecución se extiende hasta que el usuario decida darse de baja.*

*En los servicios gratuitos si bien no existe un medio de transacción expreso el dinero en su reemplazo se hallan los datos que brindan los usuarios los cuales le sirve al proveedor mediante análisis a través de algoritmos para generar perfiles de usuarios lo cual es licito siempre que cumpla con su obligación de*

*brindar información relevante, oportuna, veraz, suficiente, de fácil comprensión y fácilmente accesible debiendo ser brindada en el idioma del usuario.*

*Estos últimos son los que pueden llegar a plantear mayores problemas, ya que la gratuidad suele llevar aparejada la pérdida de privacidad. Además, como toda herramienta en manos humanas, puede ser usada con fines lícitos o ilícitos, legítimos o ilegítimos.*

*El desarrollo de aplicaciones que generan plataformas de intercambio de datos y contenidos, y el nacimiento de la web 2.0. y de los sitios web colaborativos (blogs, wikis y redes sociales) en la que los usuarios de la red dejan de ser meros "consumidores" para transformarse en Prosumidores generadores de contenidos lo que acentúa más los riesgos para la privacidad, particularmente en las redes sociales, en la que los datos personales pasan de ser un elemento accesorio necesario para convertirse en el elemento clave para el funcionamiento de las mismas. su funcionamiento.*

*Para que los diferentes usos y finalidades de Internet se consoliden y se generalicen, los usuarios necesitan contar información relevante, oportuna, fácilmente accesible y de fácil comprensión que le genere confianza entre otros factores. Y esa confianza sólo puede ganarse protegiendo y garantizando la privacidad y la seguridad de los mismos. En una anterior Declaración ya se hizo hincapié en los diferentes tipos penales que se dan en Internet y ahora toca analizar los problemas que afectan a la privacidad en Internet desde la perspectiva de la protección de datos personales de sus usuarios. Como venimos recordando a lo largo de todas las Declaraciones presentadas, al existir un componente de internacionalidad y universalidad en la red, las diferentes legislaciones nacionales por sí solas no pueden dar una respuesta adecuada a estos problemas y por ello, deben unificarse para evitar que estas empresas y sus servidores no se ubiquen en países que no ofrezcan niveles adecuados de protección en materia de privacidad.*

*Un primer uso de Internet es el comercio electrónico. La posibilidad de poder comprar desde cualquier lugar y a cualquier hora tiene un gran potencial de crecimiento. Pero una de las causas que ralentizan el mismo es la falta de seguridad que perciben sus potenciales usuarios, sobre todo si la empresa con la que queremos contratar se encuentra ubicada en otro Estado y por ello se encuentra sometida a una*

*legislación sobre privacidad y comercio electrónico que desconocemos, o que ni siquiera existe. El usuario tiene que tener confianza de quien está detrás de ese sitio Web y del uso que va a dar a sus datos personales. Es por ello que las diferentes legislaciones deben exigir la implantación de avisos legales ubicados en lugares visibles de las páginas webs que de forma clara y precisa nos informen de quien está detrás de ese dominio y que cuenta con todos los permisos y autorizaciones necesarios para el ejercicio de esa actividad, como podemos contactar con él, que garantías legales tenemos como consumidores, y que piensa hacer con nuestros datos personales y de que manera podemos oponernos a ese tratamiento en un futuro. De la misma manera, las diferentes legislaciones deben imponer ciertas obligaciones a los responsables de estos tratamientos en lo que no se ve por parte el usuario, pero que puede darle confianza el saber que ese responsable tiene obligación de cumplir unos requerimientos legales sobre seguridad en lo tratamientos, ejercicios de derechos, encargados de tratamiento, transferencias internacionales de datos, cesiones de datos, deber de información y consentimientos. En las distintas legislaciones resulta fundamental reforzar, por tanto, la idea del control sobre los datos de los cuales se es titular, lo que conlleva a favorecer la protección de los datos de carácter personal frente a toda intromisión de terceros, sean éstos públicos o privados, y por tanto, establecer las condiciones bajo las cuales estos últimos podrán efectuar legítimamente el tratamiento de tales datos.*

*Conforme a los lineamientos internacionales, la regla general debe ser un consentimiento previo, inequívoco e informado para el tratamiento de datos personales. Lo que interesa es que las formas del consentimiento estén acordes a los usos y costumbres de los usuarios de Internet y a la vez provean a éstos la información suficiente para que tomen una opción – expresa o a través del mero uso – debidamente informada.*

*Todo proveedor de servicios debe brindar información relevante, oportuna, veraz, suficiente, de fácil comprensión y fácilmente accesible debiendo ser brindada en el idioma oficial del país de cada usuario agregar además que no solo se debe cumplir con el mero hecho de brindar información de manera textual si no que a su vez se presente a través de animaciones al momento de entablar la relación de consumo y en el transcurrir de la misma enviando al correo electrónico del usuario la información relevante para hacer valer sus derechos.*

*El Cloud Computing es otro de los servicios (gratuitos o de pago), que puede incrementar su volumen de negocio en los próximos años. La posibilidad de alojar datos y que estos sean accesibles desde cualquier lugar o dispositivo con conexión a Internet, ofrece posibilidades desconocidas aún. Estos servicios no tienen ningún impedimento técnico a la hora de plantearse su contratación con un prestador de otro país, pero si no se armonizan las diferentes legislaciones imponiendo unas obligaciones a estos encargados de tratamiento en lo que respecta a la limitación de usos de esos datos, implantación de medidas de seguridad o derecho a la portabilidad, si que pueden existir impedimentos de tipo legal a la contratación de un prestador ubicado en un país extranjero o que no exista este impedimento pero no se produzca la contratación por falta de confianza.*

*Como ya hemos reflejado anteriormente, la gratuidad suele conllevar a cambio una pérdida de privacidad. Es legítimo ofrecer un producto o servicio gratuito y pretender obtener ingresos por otras vías, pero lo que no se puede permitir es que bajo la apariencia de "falsa gratuidad" se comercie con nuestros datos a través de la construcción de perfiles de usuarios, mediante las cuales se elabore un perfil comercial basado en nuestros hábitos o preferencias y se nos bombardeen con publicidad sin habernos informado de forma clara y sencilla antes de prestar nuestro consentimiento del tratamiento de nuestros datos y la finalidad y usos de los mismos, así como de nuestros derechos respecto a los mismos.*

*Igualmente hay que garantizar la protección de los usuarios cuando se producen cambios unilaterales y sobre la marcha de las reglas del juego, a fin de garantizar que se sigan cumpliendo los principios básicos antes mencionados. Es por ello que las legislaciones nacionales deben uniformarse para evitar que los propietarios de estas redes sociales y servicios de mensajería instantánea y sus servidores no se ubiquen en países permisivos en materia de privacidad donde puedan dar rienda suelta a prácticas prohibidas por ley en otros Estados. Independientemente de donde se encuentren ubicadas estas empresas, deberían mediante avisos legales informarnos previamente al alta como usuario o a la instalación de esa aplicación en nuestro dispositivo electrónico, de una manera clara y precisa del tratamiento y usos que de van a dar a nuestros datos y de la manera de oponernos a ello. De la misma manera, si cambia la política de privacidad, se nos debería avisar con suficiente antelación del cambio, de manera que podamos*

*oponernos a ello o solicitar, en su caso, la baja del servicio o red social. Y lo que debería quedar terminantemente prohibido en todas las legislaciones es el mantenimiento de esos datos una vez que el usuario se he dado de baja y los plazos legales de reclamación judicial o administrativa han prescrito.*

*Otro problema que afecta a la privacidad de los ciudadanos o los trabajadores, son los sistemas de geolocalización instalados en los dispositivos y aplicaciones móviles. Las diferentes legislaciones deberían armonizarse obligando con carácter previo a informar sobre los tratamientos y usos previstos, dar la posibilidad de oponerse a ellos, informar sobre el modo de ejercitar los derechos reconocidos y permitir su desconexión temporal o definitiva por parte del usuario, solicitando permiso previo para su posterior activación. También se debería obligar a los fabricantes e instaladores a que por defecto dejen deshabilitada esta opción. Las diferentes legislaciones deben ser especialmente protectoras con la privacidad del menor cuando estos sistemas vayan dirigidos a ellos o puedan ser utilizados por sus padres o representantes legales como herramientas de control parental.*

*Las recurrentes informaciones en los últimos tiempos relativas a casos de espionaje en la red, así como las relativas a los llamados "delitos informáticos", han puesto en boga el derecho a la protección de datos en la red de redes. Esto se plasma en un cada vez mayor celo de los usuarios en el uso de Internet a la hora de compartir información, y gracias a esta labor divulgativa de los medios los ciudadanos identifican con mayor claridad este derecho y sus implicaciones y riesgos, aunque la información aún es insuficiente, como recientes estudios señalan.*

*Por tanto, urge que las autoridades nacionales e internacionales, entidades publicas y privadas, asociaciones de consumidores hagan un esfuerzo en materia de formación y concienciación de los usuarios sobre la seguridad de la información en Internet, como medida preventiva fundamental a fin de que el usuario sea consciente de los riesgos y se convierta en el principal garante de su privacidad.*

*Muy especialmente en el caso de padres y menores, ya que estos últimos acceden desde edad muy temprana a la red, y son el colectivo más vulnerable y susceptible de sufrir ataques a su intimidad.*

*Todos los servicios antes mencionados, sean gratuitos o pagados significan un flujo transfronterizo de datos personales, materia que debe ser recogida en las distintas legislaciones. Justamente una adecuada normativa resulta clave para el desarrollo de mercados emergentes tales como el de offshoring o servicios globales*

*Por otra parte, es indiscutible que actualmente el acceso a las políticas de privacidad, avisos legales o condiciones generales de contratación o uso de los sitios web es marginal. Los usuarios cuando entran en un portal, suben un vídeo, comparten un archivo, o compran un producto, no conocen el tratamiento, uso o cesión de sus datos personales, la cesión o no de la titularidad o uso del contenido, o los derechos que le asisten como consumidor.*

*En definitiva, no se presta el consentimiento basado en una información clara y confiable, por lo que tal y como hemos ido apuntando, es necesario la realización de estándares internacionales que garanticen la protección eficaz de estos derechos*

*Este estado de cosas obliga a proponer estándares internacionales compartidos que garanticen la transparencia y el acceso a la información de forma clara y comprensible.*

*En relación a este tema, otro de los problemas mayores que se da en Internet es que es muy fácil entrar y muy complicado salir. De igual forma, una vez que el contenido entra, se pierde el control sobre el mismo, siendo cualquier usuario de la red potencial visualizador o descargador del mismo. Deviene por tanto necesaria una unificación legislativa para poder acceder, modificar, trasladar, retirar u oponerse al uso de contenidos, independientemente del lugar donde se encuentre ubicado el servidor y el particular o la empresa que lo ha subido. En cuanto a la eliminación de datos de la red, siempre que por la tipología del dato no exista una obligación temporal de conservación, o que no pueda ser requerido por un juzgado, tribunal o administración pública en el ejercicio de sus competencias, o que esa retirada atente contra la libertad de expresión o de información, ese dato o información debería ser eliminado mediante una simple solicitud de su titular . Se deberían unificar y clarificar estos criterios o supuestos de retirada, así como avanzar en el reconocimiento y ejecución de resoluciones judiciales de manera que el afectado*

*sólo tenga que actuar en los tribunales de su país de residencia sin necesidad de acudir a multitud de jurisdicciones.*

*En definitiva, se debe garantizar y brindar las herramientas necesarias para que los usuarios tengan un control del tratamiento de sus datos y de los contenidos publicados en la red.*

*Otro de los riesgos que presenta Internet en cuanto a la privacidad son las grandes bases de datos que se almacenan en sitios web o grandes plataformas tecnológicas en red, como las relativas a los usuarios de consolas de videojuegos, los perfiles de las redes sociales, los datos almacenados en las bases de datos de sitios web de grandes bancos, compañías o entes públicos, etc. No pocos casos han sido noticia de ataques cibernéticos a estas plataformas, con fugas de información, robo de datos, publicación de información confidencial, phishing, y todo tipo de delitos informáticos. Por tanto, es necesaria garantizar la seguridad tecnológica de la estructura donde se alojan todas esas inmensas "bolsas" de datos personales e información confidencial, para minimizar los riesgos de estos ataques.*

*En relación con este punto, hay que subrayar como fundamental la colaboración de estas grandes plataformas, junto con los prestadores de servicios de Internet, con la policía y cuerpos de seguridad nacionales e internacionales, estableciendo canales de comunicación rápidos y eficaces para atajar de forma inmediata los ilícitos que pudieran llevarse a cabo. Es necesario en este punto la existencia y el reforzamiento de brigadas especializadas en el ámbito tecnológico en las fuerzas y cuerpos de seguridad de los estados.*

*Asimismo las legislaciones deben unificarse regulando los supuestos en los que un Estado puede acceder a la información que los usuarios (residentes en ese país o en terceros estados) de Internet tienen alojados en los servidores de sus empresas. De la misma manera que para la intervención de las comunicaciones telefónicas, la mayoría de los países democráticos obligan a la necesidad de contar con autorización judicial, el acceso a los datos y comunicaciones de los usuarios de Internet debería contar con la preceptiva autorización judicial. Esa autorización judicial debería ser individualizada y ser limitada en el tiempo, evitándose así la tentación de realizar espionajes generalizados y masivos, como hemos tenido la ocasión de comprobar.*

*El o los organismos encargados de control o fiscalización del tratamiento adecuado de los datos personales deben promover políticas públicas para educar o instruir a las personas con el fin de que tomen control de su seguridad y privacidad. En la actualidad, uno de los principales temores de los usuarios es que sus datos personales se filtren y sean utilizados de manera maliciosa o que terceros accedan a sus datos y/o cuentas sin su consentimiento. Los organismos de control tienen la responsabilidad de educar a la población sobre buenas prácticas de seguridad digital.*

*El lenguaje informático común conocido como el Internet, en estrecha unión con la liberalización de las comunicaciones y los avances tecnológicos, ha supuesto una sacudida socio-cultural de proporciones similares a la que en sus tiempos significó la Revolución Industrial. Nos hallamos, en fin, sumergidos en la sociedad de las nuevas tecnologías, cuyos avances hacen posibles los flujos de información en dimensiones desconocidas hasta la fecha. Los bastidores de la red permiten la marea constante de una revelación de hechos que, urdida en la globalización, trasciende mucho más allá de las fronteras de cada territorio y como no podía ser de otro modo, la aparición de las redes digitales ha conmovido, también, los pilares de la dignidad humana. La información concerniente a la vida particular de los individuos se enfrenta, cada vez con mayor energía, a las transmisiones en línea por redes telemáticas como Internet; lo que comporta una potencial agresión a la esfera privada de la persona, pues resulta incuestionable la facilidad de recolectar y comunicar datos, que pueden ser capturados por los internautas en las redes y transmitidos con gran sencillez de un usuario a otro. Ya no sirven, las viejas estructuras burocráticas. La nueva sociedad exige la redefinición de los conceptos, actitudes y habilidades de los dirigentes políticos y de la función pública.*

*La protección de datos debe estar presente en las agendas internacionales, siendo un tema de relevancia actual y especialmente en el futuro, dado la expansión del llamado entorno digital, principalmente del fenómeno Internet y dentro de ella, las llamadas redes sociales, debiéndose enfatizar en la necesidad de restaurar las relaciones de confianza y reformar los procedimientos de consentimiento, todo en aras de una mayor protección de la intimidad, el honor y la privacidad de las personas, garantizando sus derechos.*