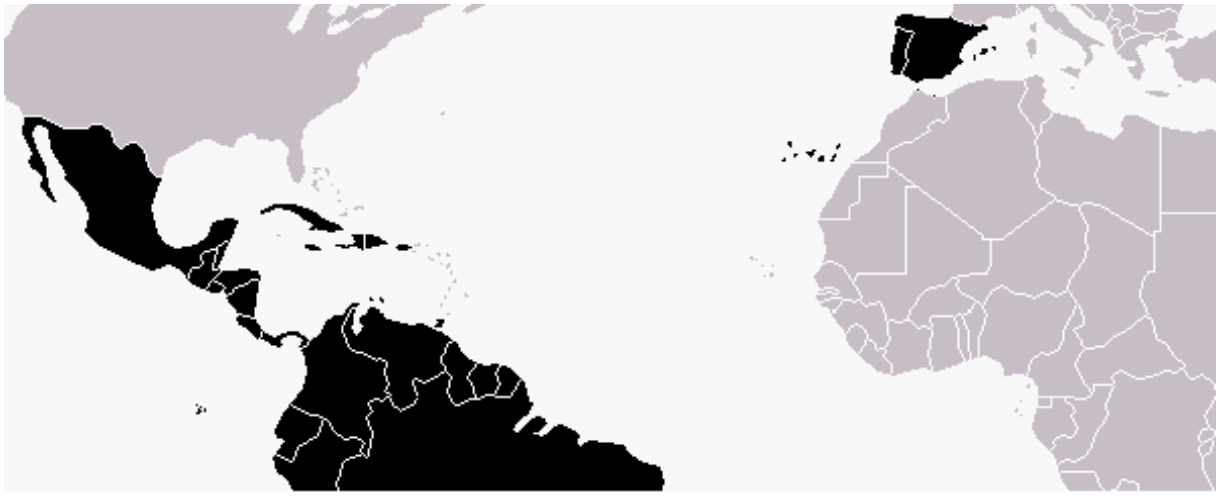

Declaración de Riobamba, hacia la unificación de criterios y medidas de seguridad para una efectiva protección de datos [1]

Desde la evolución del ser humano, el acceso y la creación de la información ha sido constante, es así que al verse basta y extensa en el mundo entero, ha necesitado de un cierto cuidado sobre todo por el tipo de información que se percibe y recepta entre intercomunicadores, con más motivo la de carácter sensible, por lo que para la protección de la información y el dato, y con el pasar del tiempo, se han creado medidas que puedan asegurar su privacidad y legitimidad frente a terceras personas que quieran hacer un mal uso de esta o inclusive apoderarse con fines pecuniarios.

La ausencia de una cultura en seguridad de la información por parte de administraciones públicas, empresas y ciudadanos es palpable. Ello origina riesgos de seguridad de los datos ante la no adopción de medidas que precautelen su seguridad, así como para evitar la obtención de ventajas derivadas de la implantación (mejora de la imagen corporativa, aseguramiento de la continuidad del negocio ante eventos relacionados con la seguridad de la información…).

[1] *La Declaración de Riobamba, hacia la unificación de criterios y medidas de seguridad para una efectiva protección de datos, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada en la Universidad de Chimborazo (ciudad de Riobamba de la República del Ecuador), el 29 de marzo de 2014, por Alexander Cuenca Espinosa, en el transcurso de la Inauguración del Curso de Formación y Especialización para Peritos Profesionales en Ecuador.*

La Comisión Europea en el documento «La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI», de 25 de enero de 2012, utiliza la expresión "nuevo y complejo entorno digital actual" para referirse al contexto en el que se le plantean retos a la protección de los datos de carácter personal, una expresión que también resulta de aplicación a los retos que, con carácter general, se le plantean a la seguridad de las tecnologías de la información y la comunicación.

Esa complejidad a la que hace referencia la Comisión Europea está formada por diferentes variables, todas y cada una de ellas a su vez con sus complejidades:

1. La rápida evolución de las tecnologías y de su uso social: en el desarrollo e implementación de los productos y soluciones tecnológicas, pero también en su uso, se prioriza la funcionalidad, por encima de otros criterios, como el de la seguridad de la información, que suele descuidarse o dejarse en un segundo término; ese acelerado ritmo de propuestas tecnológicas y de servicios difícilmente pueden ser asumido por los legisladores y reguladores, al menos con los mecanismos normativos tradicionales.

2. La extraordinaria capacidad de procesamiento de la información: tanto desde la perspectiva cuantitativa (volumen de información), como cualitativa (diferentes tipos de informaciones), con efectos positivos, pero también con impactos negativos, ya que esas capacidades también se ponen al servicio de lo ilícito.

3. El hecho de que la información tenga un valor económico: la información es un objeto susceptible de comercialización, la compra/venta de información tanto de manera lícita como ilícita, constituye una actividad más de negocio, formando ya parte esencial y motor de la economía del siglo XXI, donde el desarrollo de la sociedad de la información y progreso económico van estrechamente unidos, pero en paralelo también se ha incorporado al catálogo de actividades delictivas de grupos altamente organizados y profesionales. Los "ciberataques" masivos, sin otro objetivo que entorpecer o importunar, han pasado a la historia, ahora se trata de ataques directos, absolutamente dirigidos, que tienen objetivos e intereses claros y definidos. Hay que destacar que incluso personas en el mercado de la Deep Web venden sus conocimientos para el hurto de información a terceras personas como industrias, corporaciones, para otras en ventaja de la información que poseen pueden

generar más que las empresas de su competencia, en lo que se denomina "competencia desleal", más por la atribución de tener información adicional ilícitamente.

4. La confrontación entre la seguridad pública y los derechos y libertades individuales: las tecnologías, y especialmente Internet, están mermando sustancialmente los logros en derechos y libertados conseguidos a lo largo de varios decenios, la intromisión en la vida privada, la alteración de la presunción de inocencia o la censura de Internet, son tan solo unos ejemplos de las actividades lideradas por los Estados cuando actúan como garantes de la seguridad pública o nacional.

5. La globalidad del entorno digital: lo que comporta, a la práctica, la transformación del concepto de territorialidad y de las fronteras entre estados, con las dificultades que ello conlleva para la aplicabilidad de las normas, la determinación de la jurisdicción competente y la ejecución de las decisiones de las autoridades, aunque todo ello solo sea, en estos momentos, "la punta del iceberg".

Si a esa complejidad le añadimos los diferentes actores que despliegan su papel en ese escenario, esa complejidad se ve claramente amplificada. Las empresas y grandes corporaciones con sus intereses empresariales, los ciudadanos de manera individual o colectiva, lo que incluye a los menores, los grupos de presión de diversa índole y tendencia, los estados con sus servicios de inteligencia y cuerpos de seguridad, la delincuencia organizada, los grupos de activistas, y otros actores, todos ellos actuando en el mismo plano pero con diferentes intereses y capacidades. Incluso, se está produciendo un cambio en los hábitos de la criminalidad , y del espionaje y "guerra" entre países. Así, sobre el primero, crece la criminalidad en la red bajando la que se produce en el mundo real; sobre la segunda, se habla de de "ciber-guerra".

A toda esa magnitud del entorno digital se une el hecho de que las relaciones laborales, interpersonales, educativas, de ciudadanía, de negocio, etc., se despliegan tanto en el plano presencial como en el plano lógico o virtual, de manera que la realidad finalmente está formada por la suma de ambos espacios, lo que sucede en el plano virtual tiene consecuencias en el plano físico, y viceversa.

Si a todo lo antedicho le sumamos una generalizada falta de cultura de seguridad de la información, especialmente entre la ciudadanía, todo y que no exclusivamente, ya que también

afecta a las empresas y al sector público, que con carácter general no son conscientes de los riesgos que para sus actividades, incluso para su supervivencia, conlleva la no implantación de las medidas de seguridad de la información adecuadas, es decir, basadas en la evaluación y gestión de los riesgos a que están sujetos sus sistemas de información, junto con el hecho de que tampoco dedican demasiados esfuerzos a la gestión de su seguridad, da como resultado un panorama, al menos desde la perspectiva de la seguridad de la información, cuando menos, caótico.

Estamos ante un cambio de paradigma de las amenazas a que están expuestos los sistemas de información, lo que hace preciso un cambio de actitud, si bien los principios tradicionales de la seguridad de la información siguen siendo vigentes deben ser potenciados y reforzados para minimizar los impactos negativos.

Los impactos negativos o mínimos se potenciarían educando a la ciudadanía en los lineamientos de la Sociedad de la Información brindando herramientas para que estos puedan proteger sus datos del entorno digital que hoy en dia compromete y rodea al menos a un cuarto de la población mundial quien tiene acceso a algún tipo de tecnología en donde su información personal puede ser vulnerada.

Cuestiones tan simples como la implantación de medidas de seguridad preventivas, reactivas y de recuperación, es decir, saber cómo actuar para protegerse antes, durante y una vez se ha producido el incidente, no forman parte de las prioridades, ni tan solo de la cultura, de la mayoría de los actores que desarrollan sus actividades en plena sociedad de la información.

Las consecuencias negativas de no tener en cuenta, con suficiente antelación y de manera planificada, como proteger los sistemas de información resultan evidentes, lo mismo de evidentes deberían ser los impactos positivos derivados de la capacidad para prevenir y reaccionar antes de que se produzcan los ataques a los sistemas de información, y de recuperar la situación previa al incidente de seguridad, con las mínimas afectaciones posibles.

La seguridad de la información debe ocupar por tanto el lugar que le corresponde, debe estar presente, junto con los aspectos funcionales y de negocio, en las primeras etapas de desarrollo de las soluciones y productos tecnológicos, y de sociedad de la información, pero también debe gestionarse de manera continuada y adecuada. La apuesta e impulso por el privacy by desing, es decir, que el

producto o servicio desde su gestación esté empapado de privacidad ofrecen gran utilidad ya que uno de sus pilares debe ser la seguridad de los datos.

Cada empresa esta constituida por diversos elementos, cada uno de ellos son los que le otorgan la eficacia y sostenibilidad necesaria para que la empresa pueda mantenerse estable. Dentro de estos activos, necesariamente se debe hablar de la seguridad de información, esto en el entendido de que las empresas y su "saber industrial", su "saber como" y "datos privados sobre sus clientes" es traducido y plasmado en bits, es decir, su manera de comportarse y con quienes se comportan las empresas, se encuentra almacenado de manera digital ya sea en sus mismas oficinas, o en un servicio de cómputo en la nube externo.

Es precisamente este elemento de información, aquel que podría reflejarse como el esqueleto del modelo de negocios de la empresa, es tal la importancia de esta información, que de ser obtenida de manera ilegítima, podría significar que la copia y simulación de los modelos, al igual que la desacreditación de la empresa, por la fácil obtención de datos privados de su cartera de clientes.

Mientras más importante sea un elemento en la empresa, mayor debe ser la tutela que reciba por la misma, al momento en que se comprende el valor de la información y su fragilidad en cuanto a su destrucción, manipulación y acceso indebido, es cuando las empresas deben velar por la implementación de medidas de seguridad.

Cuando pretendemos respetar las normativas de privacidad de los distintos Estados Iberoamericanos, lo natural es acudir a la legislación propia de cada territorio y comprobar cuales son los principios rectores y las medidas de seguridad aplicables. Pues bien, ese listado de medidas de seguridad tanto técnicas, organizativas como jurídicas, se deben implementar en toda entidad que trate datos de carácter personal en aras de proteger los mismos. Son medidas que deben ser homogéneas para permitir la interoperabilidad de protocolos de seguridad, redes y sistemas en un mundo globalizado. Estas medidas además no tienen en cuenta la dimensión y especificidades de las organizaciones basándose, en su mayoría, únicamente en la sensibilidad de la información personal tratada.

Además, no debemos considerar que la adopción de las medidas de seguridad es únicamente un trámite impuesto por la normativa, sino que su función principal es asegurar los activos de la organización, que no son otros que los datos de las personas.

Pero la tendencia de las legislaciones de privacidad es alcanzar una mayor personalización al proteger la información personal de los individuos que se relacionan con las entidades y conseguir que éstas controlen y resuelvan más eficazmente las posibles fugas de información. Para lograr este segundo objetivo un ejemplo es Europa, en el nuevo Reglamento que se está preparando, encontramos la obligación de comunicar a las autoridades de control las brechas de seguridad que se produzcan en un periodo de tiempo relativamente corto, 72 horas. Esta obligación de notificar es incluso posible que se extienda a los afectados por la misma como ya ocurre con los operadores de servicios de telecomunicaciones. De esta forma, se busca una proactividad, de manera que los afectados puedan adoptar las medidas que fuesen necesarias para proteger sus datos (como por ejemplo, cambiar una contraseña si ha habido una fuga de las mismas que afecten a gran cantidad de usuarios), así como una transparencia en la gestión por parte de las organizaciones. Por lo tanto, la tendencia de introducir medidas destinadas a favorecer el principio de accountability o rendición de cuentas por parte de empresas, corporaciones o administraciones públicas, debería generalizarse ya que obligan a tomar en cuenta la seguridad de los datos.

Por otra parte, se intenta personalizar las medidas a ejecutar estableciendo la obligación de elaborar las llamadas "evaluaciones de impacto sobre privacidad" (Privacy Impact Assessment). Se trata de un informe que al igual que la Privacidad por Diseño, también está previsto en el futuro Reglamento de Protección de Datos de la Unión Europea y se encuentra vigente ya en algunos países sobre todo de influencia anglosajona. Así, por ejemplo, el organismo supervisor de protección de datos en el Reino Unido el ICO (Information Commissioner´s Office) ha elaborado varios manuales en los que se explica cómo elaborar una PIA. En España la Agencia Española de Protección de Datos está trabajando en esa misma línea aunque de momento no será obligatorio realizarla. Con este panorama y siendo una medida que refuerza la seguridad de los datos se hace necesario su generalización en las diferentes legislaciones sobre privacidad y seguridad de la información.

Esta "declaración de impacto" es una obligación similar a las evaluaciones de impacto ambiental exigidas en las distintas normativas. Una declaración de impacto no debe ser una mera verificación de cumplimiento normativo. Consiste en la elaboración por parte del Responsable del Tratamiento de un análisis de riesgos con la finalidad de determinar si el tratamiento que llevará a cabo entraña riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines. Un hecho a destacar es que las autoridades de control podrán conocer estas evaluaciones de impacto puesto que deberán hacerse públicas las conclusiones por el equipo encargado de realizarlas, por ejemplo por medio del sitio web de la organización.

Las evaluaciones deberían contener, como mínimo una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a los riesgos y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales.

Además, para realizar un PIA es importante que exista una colaboración total en la organización, de forma que participen todos los agentes implicados (por ejemplo, el departamento jurídico junto con el departamento que haya desarrollado una aplicación).

El responsable del tratamiento tiene que recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

Otra buena práctica aun sin ser obligatoria puede ser la autorregulación por parte de la entidad adoptando un sistema de gestión de seguridad de la información ISO 27001. Esta medida reforzaría uno de los pilares de una Declaración de Impacto, a saber la seguridad de los datos, eso sí teniendo presente que los riesgos de incumplimiento normativo deben ser evitados o eliminados, nunca asumidos, como así se indicó en la 6ª Sesión Anual Abierta de la Agencia Española de Protección de Datos.

Desde un punto de vista jurídico, la adopción o no de las medidas de índole técnica y organizativas destinadas garantizar la seguridad de los datos tiene unas claras consecuencias.

Así nos encontramos ante una normativa de privacidad relativamente joven en todos los países de Iberoamérica. Este hecho provoca el desconocimiento de los preceptos que conforman las mismas. Un problema, sin duda, en el momento de implementar las obligaciones recogidas, pero que se acrecienta cuando una organización recibe una sanción establecida en dichas normativas por la desestabilización económica que puede sufrir la entidad.

Para garantizar el adecuado tratamiento de los datos personales, uno de los elementos más importantes para cumplirlo y alcanzarlo son las medidas de seguridad, las cuales y como encontramos en diversas legislaciones iberoamericanas, no solo se refieren a elementos técnicos o informáticos, sino que se refieren también a elementos administrativos o físicos que permitan la protección de los datos personales y que eviten la pérdida, alteración, destrucción, acceso, uso o tratamiento no autorizado.

Ahora bien, realizando un viaje por algunas de las legislaciones que en materia de datos personales existen en Iberoamérica, nos encontramos con el hecho de que en términos generales se establece la obligación para el responsable, encargado o usuario de los archivos de datos de adopte las medidas se seguridad técnicas, administrativas o físicas, que le permitan garantizar la seguridad y confidencialidad de los datos personales, evitando con ello riesgos o usos, accesos y tratamientos no autorizados o fraudulentos.

En algunas legislaciones como la mexicana y la costarricense, se establece que para el establecimiento de las medidas de seguridad los responsables no adoptarán medidas de seguridad menores a las que utilicen para su propia información o los que sean adecuados a los desarrollos tecnológicos o mecanismos de seguridad adecuados.

Para lo anterior, el esquema de implementación de las medidas de seguridad consistirá en la adopción de ciertos elementos y características generales que se irán adecuando a las necesidades de las empresas, organizaciones o modelos de negocio de los que se trate.

Citando lo establecido en las mencionadas legislaciones de México y Costa Rica, para determinar las medidas de seguridad el responsable o en su caso, encargado del tratamiento deberá considerar al momento de determinar las medidas de seguridad aplicables a cada organización el riesgo inherente por tipo de dato personal, la sensibilidad de los datos personales tratados, el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, el número de titulares de datos personales, las vulnerabilidades previas ocurridas en los sistemas de tratamiento, el riesgo por el valor potencial (cuantitativo/ cualitativo) que pudieran tener los datos personales tratados para terceras personas no autorizadas y los factores que puedan incidir en el nivel de riesgo o que provengan de otra legislación aplicable al responsable.

Una vez definidas las medidas de seguridad por parte del responsable, para garantizar su cumplimiento, ejecución y seguimiento, a su vez, el responsable deberá considerar acciones tales como la descripción detallada del tipo de datos tratados y almacenados, el inventario de datos personales, sistemas de tratamiento e infraestructura tecnológica utilizada, análisis de brecha (diferenciación entre medidas de seguridad existentes y las faltantes) y el plan de trabajo para implementar las medidas de seguridad faltantes (análisis de brecha), entre otras.

Adicional a lo anterior, México, por ejemplo, remitió las Recomendaciones en materia de seguridad de datos personales y mediante las cuales, se exhorta a los responsables y en su caso,

encargados, para que adopten un Sistema de Gestión de Seguridad de Datos Personales basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).

Con dichas Recomendaciones se pretende facilitar a los responsables el contar con una guía que les permita mantener vigente el cumplimiento de la legislación y fomentar las buenas prácticas en materia de datos personales.

Por otra parte, nos encontramos otro tipo de legislaciones que catalogan los datos personales o las medidas se seguridad en niveles y en base a los mismos, establecen o enuncian los diferentes parámetros o elementos que permitan garantizar la seguridad de los datos personales.

Ejemplo de lo anterior lo encontramos en la legislación argentina, la Disposición 11/2006 sobre las Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados, se clasifican las medidas de seguridad en tres niveles: básico, medio y crítico (aplicable a archivos, registros, bases y bancos de datos personales sensibles).

Sigue un sistema similar en cuanto a la implementación de las medidas de seguridad, es Perú, ya que tanto en el Reglamento de la Ley de Datos Personales como en la Directiva de Seguridad de la Información, establecen diferentes niveles de datos personales y sus correspondientes medidas de seguridad, donde se establecen los lineamientos para determinar las medidas de seguridad mediante un sistema de categorización más complejo y detallado que en el caso anterior, para cada grupo se consideran variables sobre el tipo de dato; así como variables cuantitativas relacionadas con el número de personales respecto de las cuales se maneja la información y el número de datos personales que son contenidos o tratados en cada base de datos, estableciéndose los niveles básico, simple, intermedio, complejo y crítico.

De manera relacionada a las medidas de seguridad, las distintas legislaciones contemplan el hecho de que en caso de que lleguen a existir vulneraciones a la seguridad durante el tratamiento de los datos, los responsables tendrán la obligación de informar de manera inmediata al titular (en el caso de México, Uruguay y Costa Rica) o a la autoridad competente (en el caso de Colombia). Con la finalidad de que el titular pueda tomar las medidas necesarias o prudentes en defensa de sus derechos y/o de que las autoridades puedan ejercer las acciones que permitan efectuar las investigaciones o procedimientos judiciales o administrativos que correspondan.

Las sanciones que más proliferan son las administrativas a lo largo de los textos legales, y en caso de no implementar alguna de las medidas de seguridad, las sanciones alcanzan sumas

económicas muy elevadas, llegando a poner en jaque la estabilidad del negocio del que las recibe. En todo caso, no debemos olvidar que la normativa europea permite que en la vía jurisdiccional ordinaria una persona reclame a una entidad privada una indemnización cuando considera que la vulneración de sus derechos le ha provocado daños y perjuicios. En el caso de las entidades públicas, como norma general, la indemnización se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

En tanto el tratamiento de datos personales afecta a la esfera más íntima de las personas y su protección viene recogida en la mayor de Constituciones iberoamericanas, en aras a una mayor defensa del derecho al honor, a la privacidad, al buen nombre y la intimidad de las personas, se debe dotar el ordenamiento penal de instrumentos preventivos y coercitivos que eviten conductas delictivas que pongan en juego la seguridad de la información, ataques, tráfico de datos, accesos no autorizados, suplantación de identidades o utilización de la información con finalidades al margen de la ley.

Por otra parte y desde el punto de vista administrativo, existe la figura del apercibimiento que se ha introducido en los últimos tiempos con el objetivo que las instituciones reaccionen y cumplan con las medidas de seguridad bajo la amenaza de sanción económica.

En cambio, en algunos Estados como México sí que se establecen sanciones penales o privativas de libertad en caso de no cumplir con las obligaciones fijadas en la normativa de protección de datos. Alcanzando hasta los diez años de cárcel en los casos más graves.

No cabe duda que en innumerables ocasiones las sanciones económicas han sido desproporcionadas y no han tenido en cuenta la dimensión de la entidad que las recibe. Se han debido cerrar negocios por el hecho de no poder afrontar la cuantía impuesta por una autoridad de control, por ello la tendencia actual es a modular la sanción en relación al volumen de negocio de la entidad y, sobretodo, atenuarlas en base al espíritu y preocupación empresarial en la implementación de medidas de seguridad de protección de datos personales.

La seguridad en toda la amplitud de la palabra, debe hacer referencia a otorgar intangibilidad al activo, la certeza que no será destruido ni dañado, o accedido por terceros no autorizados. La seguridad que ha de buscarse dentro de una institución no debe ser sólo la seguridad informática, sino la seguridad de la información, en el entendido de que una cultura de seguridad debe ser

cultivada de manera interna y en todos los niveles tanto administrativos como ejecutivos, no siendo confiada sólo a dispositivos electrónicos programados.

Si bien la información es un activo de la empresa, y la fuga o vulneración del mismo supone, grandes pérdidas monetarias, no se puede olvidar que la implementación de medidas de seguridad, es una inversión cuyas ganancias son vistas a largo plazo. Estos beneficios se traducen en generación de confianza, imagen corporativa, optimización de recursos y capital humano y trazabilidad de la información entre otros.

Mediante la delimitación de perfiles de usuarios en el acceso a la información conforme a las funciones que desarrollan y su puesto de trabajo se optimiza el tiempo dedicado, asignado a cada empleado los recursos necesarios para desarrollar su trabajo, con lo que conseguimos por un lado optimizar el tiempo real de trabajo (ya que sólo podrá acceder a la información precisa para sus funciones) y por otro, un uso racional de lo recursos. Como consecuencia de la adecuación de los procedimientos y sistemas en protección de datos, se pueden descubrir procesos innecesarios, redundantes, o ineficientes que pueden mejorarse sustancialmente con muy poco esfuerzo.

Proteger la información adoptando medidas de seguridad, debe seguirse de una mayor educación, cultura y prevención, que son los lineamientos más avanzados en materia de seguridad, estos son controles regulares que se realizan al personal de la empresa, para ver que tipo de actos cometen y si es que estos podrían traer consecuencias desfavorables para la seguridad.

La libertad de expresión, el honor, la intimidad, la privacidad y la protección de datos personales, como derecho autónomo, e independiente, deben estar equilibrados con el concepto de seguridad, tanto en materia empresarial como pública.

La seguridad de los datos personales implica un delicado balance de distintas cuestiones, tales como el nivel de riesgo, la cantidad de datos protegidos por persona, el número de personas cuyos datos personales están siendo tratados, los posibles daños o amenazas, costos financieros y de eficiencia de las medidas de seguridad implementadas para reducir el riesgo y las que se relacionen con las características específicas de la industria de que se trate, tal y como lo mencionaba Daniel Solove.

La integración económica y social resultante del establecimiento y funcionamiento de un mercado globalizado, ha implicado un desarrollo notable de los flujos transfronterizos de datos

personales entre distintos agentes públicos y privados establecidos en diferentes países. Este flujo de datos se ha visto favorecido por factores como el avance de las tecnologías de la información y, en particular, el desarrollo de Internet, que facilitan considerablemente el tratamiento y el intercambio de información, y que permiten compartir recursos tecnológicos, centralizar determinadas actividades y procesos, y abaratar costes en la prestación de servicios por la propia empresa fuera del país en el que se encuentra establecida.