



Declaración de Ciudad de Panamá, hacia la unificación de criterios y garantías para la protección de la identidad digital y el derecho al olvido ¹

El mundo virtual de Internet y las Redes Sociales posibilitan un sinfín de interconexiones y comunicaciones ilimitadas y heterogéneas que logran efectos de conectividad e interacción social antes impensados, pero que también logran traspasar límites físicos, psicológicos, emocionales, económicos, culturales, políticos, laborales, educativos y sociales, perdiendo el protagonista del mismo, el ser humano, el control sobre sus acciones en la Red.

Su Identidad como persona se ve transformada en lo que se denomina “Identidad Digital”, un espacio virtual donde la subjetividad de los individuos da lugar al surgimiento de una identidad en entornos virtuales anónimos, en donde los individuos suelen jugar roles diferentes a los de su vida real. En este contexto, se establece un fuerte vínculo entre las estructuras psicológicas y los procesos sociales que conforman y atraviesan al sujeto, es decir, entre las normas que regulan el comportamiento colectivo y las estrategias del sujeto dentro del contexto social, que permiten su articulación con la trama social.

¹ *La Declaración de Ciudad de Panamá, hacia la unificación de criterios y garantías para la protección de la identidad digital y el derecho al olvido, elaborada desde la iniciativa del Observatorio Iberoamericano de Protección de Datos, fue presentada en el Auditorio Harmodio Arias del Colegio Nacional de Abogados de Panamá, el 23 de julio, en un evento organizado por la Comisión de Derecho de las Nuevas Tecnologías del Colegio, por el Presidente del Colegio, D. José Alberto Álvarez Álvarez. En el acto también intervinieron el Dr. Rigoberto González Montenegro, así como Dña. Lía P. Hernández Pérez, como Presidenta de la Comisión de Nuevas Tecnologías del Colegio.*



La construcción de la identidad es un proceso que se establece si hay coincidencia entre posicionamiento y aceptación. En las interacciones cara a cara, es difícil pretender ser quien no es, en cambio, en el entorno de una red social es posible interactuar con otros sin que nada se revele sobre nosotros (subliminalmente muchas veces sí) construyendo la identidad deseada que en el mundo real no se puede obtener, construyendo los actores sus identidades y redundándolas, adaptándolas a sus expectativas y a los que el mundo social les demanda.

Pese a que se puede recurrir a las herramientas jurídicas para rectificar errores o reclamar daños y perjuicios, se depende de su acto voluntario, de conciencia, de decidir qué información personal o íntima va a darse a conocer públicamente y cual no.

Muchas veces los ciberdelincuentes utilizan métodos de captación ilegítima de información o software especializado en vulnerar sistemas informáticos y no hay prevención que se puede utilizar, pero en los casos cotidianos en que nuestra vida es expuesta en el mundo virtual, depende de nosotros mismos equilibrar la información personal que compartimos en la Sociedad de la Información.

La mejor herramienta de la seguridad es la prevención. Se debe tratar con un criterio razonable poder disfrutar del maravilloso mundo digital, resguardando nuestra información personal y nuestro derecho a la intimidad. El individuo debería tener protección de su persona y sus propiedades es un principio tan antiguo como la ley, pero de vez en cuando es necesario definir de nuevo la naturaleza y el alcance de esa protección. Cambios políticos, sociales y económicos, suponen el reconocimiento de nuevos derechos, y la Ley, en su eterna juventud, debe crecer para satisfacer las nuevas demandas de la sociedad. Inicialmente la Ley dio remedio a la interferencia física con la vida y la propiedad privada, y ahora le toca hacerlo con la virtual.

*Se debe lograr el equilibrio entre intimidad, privacidad, protección de datos personales, derecho al honor, a la asociación y a la libertad de expresión. Son todos Derechos Humanos, reconocidos por los Tratados Internacionales y protegidos en las legislaciones nacionales, y al alcance de la jurisdicción de los tribunales nacionales e Internacionales que conocen sobre estas cuestiones, para proteger los derechos de los ciudadanos y de la comunidad internacional en general. Los Derechos Humanos deben estar siempre presentes en todo momento y lugar, como regla del *ius Cogens*.*

Los Derechos Humanos basan sus principios en la dignidad y valor de la persona humana; así lo estableció la Convención de Viena. Crean obligaciones de los Estados con los ciudadanos directamente; y más aún que su mención en los diferentes ordenamientos legales, vale el



compromiso de los individuos con estos derechos que nos permiten relacionarnos en un entorno globalizado.

LA IDENTIDAD DIGITAL Y SU PROTECCIÓN

El concepto de Identidad debe entenderse como el conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás, concepto que llevado al ámbito digital o a la exposición y desarrollo de tal identidad en este contexto, tendremos conceptos como el que establece el Instituto Nacional de Tecnologías de la Comunicación (INTECO), “... puede ser definida como el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital.”

La formación de la identidad es algo casi inconsciente, pues se forma a medida que nos desplazamos por el ciberespacio, es así como cada contacto cuenta, al igual que cada pensamiento o acto que realizamos en nuestras diversas redes sociales.

Si bien la identidad digital, en primera instancia es generada por nosotros, se debe recordar que son otras personas también las que pueden ayudar a generar esta información, con sólo subir fotografías, comentarios y diversas actuaciones que puedan ser digitalizadas e indexadas a nuestro nombre, se estaría así contribuyendo a la formación de nuestra imagen digital.

Debe diferenciarse entre identidad digital e identidades parciales, cada identidad parcial corresponde a cada servicio o aplicación en Internet, como las redes sociales, usuarios de correo electrónico, entre otros, pero al final la suma de estas identidades parciales es lo que constituye la identidad digital.

Si bien en sus orígenes, los componentes base de la identidad estaban disponibles por medios físicos o periodísticos tales como nombres, certificados de nacimiento, títulos universitarios o profesionales, cartas de no antecedentes penales o información de notas periodísticas, sin embargo, con la aparición de los instrumentos de digitalización, del impulso en el uso de computadoras personales y con el incremento en el uso de Internet, los datos e información que componen la identidad de una persona no solamente se dispersaron con mayor facilidad, sino que se incrementaron, al grado que ahora no solo tenemos dispersada en internet información que corresponde a la identidad de las personas en lo individual, sino también de las empresas, autoridades, grupos de trabajo u organizaciones varias.



Además, con los nuevos sistemas informáticos y de comunicación, sobre todo los móviles, día a día estamos arrojando información que incrementa datos a nuestra identidad digital, tal es el caso de los datos que arrojan la geolocalización, aplicaciones que predicen nuestros gustos y deseos, las que involucran reconocimiento biométrico.

Es Internet un espacio masivo de usuarios, donde muchas veces surge el temor, de no saber con quién se está conversando, de si es o no es quien dice ser, es por ello que la identidad digital podría llegar a ser útil cuando cumple su labor de identificar a los usuarios, por ello se entiende que Internet acerca a sujetos que se encuentran tan distantes, que la única forma de conocerse es mediante estos medios.

Actualmente el que cualquier persona pueda investigar y conocer nuestra identidad digital desde cualquier parte del mundo y con ello hacer un buen o mal uso de la información, es tan importante y al mismo tiempo conlleva un gran nivel de riesgo, lo cual nos lleva a la reflexión de que deberíamos cuidarla como uno de los aspectos más preciados de nuestra vida.

Sin embargo, es preocupante cuando nuestra identidad digital sale de nuestro control, ya que la misma se va construyendo además con la información y datos que otras personas vayan generando respecto de nosotros, incluso, nuestra identidad digital llega a ser alimentada con la percepción o comportamiento que se tienen las personas con las cuales nos relacionamos, de manera que incluso existen aplicaciones, que no solo se realiza la información que las personas le proporcionan para realizar un análisis de si son susceptibles de recibir un préstamo o crédito, sino que además se toma en cuenta la información de nuestros familiares y amigos en Facebook aportan sobre nosotros, o incluso, la información que arroja el mero hecho de tener a ciertas personas como nuestros contactos o la forma en la que interactuamos con ellos.

Las redes sociales si bien son círculos meramente privados entre el usuario y sus contactos, en el supuesto que no se haya configurado bien la el apartado de privacidad pueden ocasionar que esa información pase a formar parte de Internet, al ser indexada por cualquier buscador. Esto sólo es una muestra que la imagen que se muestra sobre cada persona, no es derivada exclusivamente por la de pertenencia una red social, y no son únicamente los contactos los que pueden llegar a acceder a esta información, sino que se debe hablar de usuarios de Internet y ya no tanto de contactos de redes sociales.

La identidad digital se compone por lo menos de información proveniente de tres grandes grupos; la generada por el propio individuo, la generada por terceros y la que se genera en el contexto de las relaciones del individuo.



Uno de los problemas de la identidad digital es la posibilidad que tiene un solo individuo de generar una pluralidad de identidades, ya si bien es cierto que hay a quienes les conviene trabajar en la correcta construcción de su identidad digital para adquirir más impulso o reconocimiento social o político, también lo es que pueden existir motivos por los cuales una persona desee permanecer en el anonimato que brinda Internet, ello por distintos motivos, tales como temas de seguridad, libertad de expresión, para ocultar o disfrazar los actos o consultas de información, o cuando simplemente se tenga el interés de que tales actos no afecten la identidad principal.

Esta cuestión puede representar un problema para las empresas, las autoridades o para quienes prestan servicios vía web, o cuando la contratación de los productos o servicios se realiza mediante estos medios, ya que es muy complicado saber quién es la persona que en realidad está realizando la transacción, quedando expuestos por ejemplo a fraudes cometidos por el uso de identidades digitales falsas, los cuales en combinación con el uso de tarjetas de crédito clonadas o robadas, puede ser una herramienta muy peligrosa.

Debe tenerse en cuenta que a diferencia de la identidad en el medio físico en la cual es más fácil identificar la persona que está realizando la operación, en el medio digital tenemos el problema de la falta de conexión entre una persona determinada y una identidad digital, tan incierto puede ser que al momento de *offline* la identidad digital puede dejar de existir.

La suplantación de identidad es otro de los problemas que afecta a una de las identidades parciales del individuo, es decir, se da una afectación a una de las cuentas o aplicaciones a las cuales tiene acceso el individuo, lo cual a su vez y dependiendo del grado de intromisión y del daño causado, puede llegar a cambiar en grado considerable la identidad digital del individuo.

Lo anterior puede ser realizado mediante distintas formas, entre ellas, el uso del nombre o usuario de la persona, se genere una identidad que ridiculice a la identidad original o se haga un uso no autorizado de la cuenta, pero al final tendremos como consecuencia la afectación a la privacidad, bienes, honor o reputación de una persona.

Otros de los problemas más comunes asociados a la identidad digital son las violaciones a los derechos la privacidad, los derechos autorales, daño reputacional, sexting, bullying, entre otras actividades que van deteriorando o violentando la identidad digital de una persona, llegando a grados en los que incluso se lleguen a afectar las relaciones personales y la vida íntima de la persona.



REPUTACIÓN PERSONAL ON-LINE Y DAÑO REPUTACIONAL

Considerando la reputación como la opinión o consideración en que se tiene a alguien o algo o el prestigio o estima en que son tenidos alguien o algo. Según la definen diferentes autores “la reputación online es el reflejo del prestigio o estima de una persona o marca en Internet. A diferencia de la marca, que se puede generar a través de medios publicitarios, la reputación no está bajo el control absoluto del sujeto o la organización, sino que la ‘fabrican’ también el resto de personas cuando conversan y aportan sus opiniones.”

Debemos considerar la identificación virtual es el conjunto de datos que nos permiten diferenciarnos suficientemente del resto de personas en un ámbito concreto. Estos datos suelen ser el nombre, apellidos...

Resulta prácticamente imprescindible identificarse en redes sociales tales como Facebook o LinkedIn, cuyo principal objetivo es relacionarte y permitir que los demás usuarios te identifiquen y compartir con ellos cierta información, en el caso de la primera red, por motivos de ocio, en la segunda por motivos profesionales.

Sin embargo, cuando los usuarios no persiguen el fin de comunicarse con los demás, sino que pretenden simplemente hacer comentarios (en muchas ocasiones dañinos), prefieren esconderse tras el anonimato.

Esto genera una problemática inmensa, sobretodo cuando los comentarios dañan la reputación de personas, que no pueden defenderse frente a estas personas anónimas.

Por ello, la reputación online no es un tema que preocupe sólo a las empresas. También los particulares pueden verse afectados por suplantaciones, difamaciones o por el contenido que ellos mismos han subido a la red. El derecho al olvido pretende solucionar este problema.

Además de los métodos más comunes para dañar la imagen de una persona, como pueden ser las críticas en foros de opinión, últimamente se está poniendo “muy de moda” suplantar identidades virtuales; de hecho, este fue el principal motivo de denuncias relacionadas con Internet ante las diferentes autoridades de control en protección de datos en los últimos años.

Lo que antes se limitaba a aparecer en alguna página de contactos, porque alguien facilitaba tus datos a desconocidos, hoy se ha reemplazado por la creación de perfiles falsos en redes sociales, comunicándose el suplantador con tus amigos y conocidos, con el único fin de dañar tu imagen.

En el mundo 2.0, este tipo de suplantación es fácil, accesible y gratuita, ya que no se puede requerir y comprobar la identidad de la persona que se da de alta en una red social. Sin embargo, los suplantadores en algunos casos no son conscientes de que están cometiendo un delito de



suplantación de identidad, tipificado en el artículo 401 del Código Penal, por el cual se prevén penas de seis meses a tres años de cárcel.

A pesar de ello, las reacciones más comunes ante este tipo de delito no son las denuncias, sino las solicitudes de baja a través de las propias redes sociales y las denuncias ante la Agencia de Protección de Datos.

Las redes sociales deben estar preparadas para este tipo de controversias y disponer de formularios para denunciar los hechos. No sólo se pueden denunciar suplantaciones, también puedes denunciar si consideras que existen contenidos inapropiados en un determinado perfil.

Cuando una persona fallece, ya no sólo hay que preocuparse de las repercusiones directas en la vida real, también hay que decidir sobre las repercusiones en la red.

Internet se ha convertido en una herramienta de comunicación casi imprescindible para millones de personas, muy atractiva e interesante, entre otras ventajas, porque los servicios que ofrecen son gratuitos. Pero esa fácil accesibilidad es precisamente la que provoca que el problema surja cuando no se trata de introducir datos, sino de borrarlos, como por ejemplo, en el caso de fallecimiento de una persona.

La muerte de estas personas abre a sus familiares dos posibilidades: eliminar el perfil en la red social o permitir que se realice un homenaje en el mismo. Pero ¿están preparados los familiares para superar, no solo la muerte de una persona querida, sino también para borrar su huella?

No cabe duda que es difícil tomar cualquiera de las dos decisiones, pues en la primera te enfrentas a la repercusión que todos más tememos respecto a la muerte, el olvido, y en la segunda te enfrentas al recuerdo permanente de quien se ha ido.

Las redes sociales han previsto “el homenaje” permitiendo a los familiares directos, conservar el perfil del fallecido, con el fin de que no se produzca esa disminución masiva de usuarios de la red social.

Y el mismo derecho a conservarlo, tenemos de eliminarlo: basta con que comprobemos la política de privacidad de la red y la familia solicite la cancelación de datos de la referida persona.

Y en el caso de personas sin familia, ¿qué ocurre con ellos? En este caso deberemos iniciar actuaciones judiciales.

El problema no se produce cuando un usuario le pide al titular de una red social que cancele toda su información, sino cuando esa información ha pasado de una red a otra, y ha traspasado muchas fronteras tecnológicas y geográficas. Es entonces cuando el derecho de cancelación de datos se convierte en una ingente tarea de búsqueda desesperada, dando lugar en la mayoría de los casos a la imposibilidad práctica de eliminar de manera permanente esta huella en Internet.



REPUTACIÓN CORPORATIVA ONLINE

La identidad online de la empresa viene definida por el conjunto de información que aparece en Internet sobre la misma: datos, imágenes, registros, comentarios, etc. Dicha información engloba tanto aquellos contenidos que activamente genera la organización, como los comentarios y opiniones que los demás vierten en la corriente social. Este hecho hace que cada vez sea más importante la monitorización de la valoración que el público hace de la compañía en la Red y llevar a cabo una adecuada gestión de reputación online corporativa.

Las organizaciones difunden su imagen en Internet mediante herramientas como páginas web corporativas, blogs empresariales, perfiles y páginas en redes sociales... Más allá de lo que la propia empresa publique y dé a conocer de sí misma, la identidad digital corporativa se ve complementada con lo que los propios usuarios y clientes opinan sobre la empresa en Internet. Incluso, no es necesario que una empresa se encuentre presente en Internet, para que puedan surgir este tipo de opiniones sobre ella. Así pues, el contenido generado por terceros forma parte de su identidad digital de la misma manera que el creado por la propia empresa. La identidad digital corporativa, por tanto, puede ser definida como el conjunto de la información sobre una empresa expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha organización en el plano digital.

La Web 2.0 constituye un nuevo canal masivo de comunicación para las empresas y las redes sociales representan una herramienta mediante la cual las organizaciones disponen de un feedback en tiempo real de clientes y usuarios. En la Web 2.0 cualquier empresa o profesional puede tener presencia digital gracias a clientes y usuarios sin necesidad siquiera de tener una página web, tanto para hablar maravillas como para maldecir un servicio o producto. Es por ello, que surge un nuevo concepto: la reputación online.

La reputación corporativa es el concepto que mide cuál es la valoración que hace el público de una compañía. Podría definirse como la valoración alcanzada por una empresa a través del uso o mal uso de las posibilidades que ofrece Internet.

Al mismo tiempo que la presencia de la empresa en medios sociales (por sí misma o por la acción de terceros) le reporta efectos positivos, existen diferentes amenazas que pueden generar impactos negativos en su imagen y reputación online. Una pérdida de confianza en la marca a partir de comentarios perjudiciales sobre un producto es un ejemplo de ello. Además, el efecto multiplicador de Internet posibilita que un incidente aislado (incluso generado fuera de la Red) se convierta en una situación de difícil solución.



En este sentido, cada vez es más frecuente descubrir noticias sobre crisis reputacionales en Internet, que impactan de tal forma en la imagen de la empresa, que los efectos perduran en el tiempo. A continuación se describen las principales amenazas para la identidad digital y reputación online desde el punto de vista de la seguridad.

Otro de los problemas a los que se enfrentan las empresas es la Suplantación de identidad: la suplantación de identidad de la empresa en Internet es la usurpación de los perfiles corporativos por terceros malintencionados, actuando en su nombre. Dentro de este riesgo se contempla la creación o el acceso no autorizado al perfil de una empresa o entidad en un medio social y la utilización del mismo como si se tratara de la organización. Los atacantes crean perfiles falsos con varios propósitos, destacando el robo de información sensible de los usuarios de la empresa suplantada para la comisión de fraude online.

Registro abusivo de nombres de dominio: la amenaza se produce cuando terceros malintencionados registran uno o varios nombres de dominio que coinciden con la marca de la empresa, impidiendo a esta última utilizar dichas denominaciones en su negocio.

Ataque de seguridad DDoS: Ataque de Denegación de Servicio Distribuido, o ataque DDoS. Es el conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo, hablando en términos de seguridad informática. Para poder llevar a cabo el ataque, se requiere que varios equipos trabajen coordinadamente para enviar peticiones masivas a un servidor concreto, por ejemplo accediendo a la página web y descargando archivos, realizando visitas, etc. Así consiguen saturar dicho servidor y provocar su colapso, al no poder este responder tal flujo de peticiones.

Fuga de información: en este caso, la buena imagen y el prestigio de una entidad puede verse comprometida por el robo de información sensible y/o confidencial (como por ejemplo, datos personales de trabajadores y clientes, datos bancarios, informaciones estratégicas de la organización, etc.) y su revelación en Internet. De nuevo, el objetivo suele ser el lucro (por ejemplo, al obtener información bancaria de la empresa y sus clientes, o al extorsionar a la propietaria de los datos a cambio de un rescate), aunque también se distinguen otros motivos, como el espionaje industrial o el desprestigio a la organización.

Publicaciones por terceros de informaciones negativas: las críticas a las entidades son parte de la interacción que ofrecen las plataformas colaborativas: no solo se está en la Red, sino que se conversa en ella. El hecho de que una falta de atención, un error en el servicio, un defecto en un producto, etc., sea comentado en Internet es igualmente una información valiosa para la empresa, que puede corregir el fallo en base a estos comentarios negativos. En estos casos, la diligencia de la empresa para dar una respuesta apropiada permitirá solucionar o aliviar la corriente de crítica que se



ha generado y, en consecuencia, la recuperación de su imagen y reputación online. Asimismo, la realización de comentarios negativos o falsos sobre una organización puede tener consecuencias legales contemplándose acciones tanto civiles como penales (en caso de que la ofensa en cuestión sea considerada una injuria o una calumnia) dirigidas a proteger el honor y reputación de la empresa.

Utilización no consentida de derechos de propiedad intelectual: Estos derechos tienen una doble dimensión: permiten a su propietario su utilización e impiden que un tercero lo haga, salvo que le ampare la correspondiente licencia de uso otorgada por el primero. Si se están utilizando o comercializando a través de Internet de forma no autorizada, la empresa propietaria de sus derechos se convertiría en víctima de un delito contra los derechos de propiedad industrial y posiblemente, en un delito de competencia desleal

La empresa que haya visto dañada su reputación online tiene a su disposición una serie de herramientas legales para que su imagen se vea reparada. La Red no altera el contenido esencial de los derechos de las personas jurídicas. Sin embargo, sí existen particularidades específicas derivadas del entorno online que las empresas deben tener en cuenta a la hora de gestionar su reputación:

En primer lugar, el daño derivado del ataque a la reputación de una empresa realizado a través de Internet es difícilmente reparable de manera total. La difusión de una información publicada en la Red no tiene límites y, aun en el caso de que la información en cuestión sea retirada (por contravenir los derechos de la empresa), siempre se pueden mantener copias, pantallazos o descargas realizados antes de la eliminación.

En segundo lugar, y relacionado con lo anterior, las empresas deben considerar el llamado “efecto Streisand”, fenómeno en el que un intento de ocultamiento de cierta información en Internet resulta siendo contraproducente, ya que ésta acaba siendo ampliamente divulgada, recibiendo mayor publicidad de la que habría tenido si no se la hubiese pretendido acallar.

Las legislaciones nacionales, suelen reconocer los derechos al honor, a la intimidad personal y familiar y a la propia imagen, teniendo cabida en algunos ordenamientos jurídicos dentro del derecho al honor el derecho a la reputación corporativa. Así, reconocen expresamente que la persona jurídica también puede ver lesionado su derecho al honor a través de la divulgación de hechos concernientes a su entidad, cuando la difame o la haga desmerecer en la consideración ajena. Por tanto, las empresas y organizaciones, en defensa de su derecho al honor, deben poder iniciar acciones civiles o penales para solicitar la retirada de la Red de informaciones que produzcan un perjuicio a su reputación. En la mayoría de las ocasiones nos encontraremos ante supuestos donde entran en conflicto, de un lado, el derecho al honor de otro, el derecho a la libertad de expresión e información



EL DERECHO AL OLVIDO O CANCELACIÓN DE DATOS

Resulta indudable que hay una serie de derechos que en el entorno digital quedan más expuestos a posibles vulneraciones, y por lo tanto su desarrollo y aplicación pasan a adquirir, en dicho entorno, mayor relevancia.

Hablamos, cuanto menos, del derecho a la intimidad personal y familiar, del derecho al honor, del derecho a la propia imagen (no olvidemos que de estos tres, aunque estrechamente interrelacionados, cada uno protege aspectos distintos de la persona y a cada uno se aplican criterios jurisprudenciales diferentes), de la libertad de expresión, el derecho de información, los de propiedad intelectual y por supuesto, también, el derecho a la protección de los datos personales. Todos ellos se encuentran íntimamente ligados a la identidad digital de la persona, en la medida en que inciden directamente en la construcción de aquellos de los rasgos que caracterizan a un individuo que quedan puestos de manifiesto en la denominada web 3.0.

Internet, tal y como lo disfrutamos hoy en día ha sufrido gran cambio respecto al que conocimos en los años noventa, que era mucho más estático y unidireccional, y en el que el usuario ejercía un papel casi del todo pasivo, sin que su conducta conllevara normalmente una reacción en la red. Actualmente, en cambio, el usuario interactúa constantemente en Internet, se ha convertido en parte activa en la construcción del tejido de esta red de redes y su comportamiento puede llegar a provocar grandes reacciones. Este escenario, regido bajo el principio de neutralidad de la red y teniendo en cuenta que el acceso a Internet llega cada vez a una mayor población (como es deseable) y además por medio de más dispositivos (no digamos ya cuando vivamos el gran apogeo del Internet de las cosas), arroja unas características propias de la denominada web 3.0 que resultan de gran impacto para todos estos derechos. Tales características son: la amplificación (repercusión, alcance, rapidez y facilidad en la transmisión de la información), la accesibilidad a la información, más fácil, cómoda y barata, y la permanencia de la misma.

Ninguno de los derechos mencionados es absoluto y todos ellos, en su aplicación, encuentran su límite en otros derechos e intereses legítimos. Y en la ponderación que sea haga en el conflicto entre unos y otros, adquieren especial importancia estas características de la Internet de hoy en día.

Son varias las definiciones que se han dado, sin embargo la mayoría lo ponen en relación exclusivamente con el derecho a la protección de los datos de carácter personal, así, por ejemplo la Comisión Europea lo definió en un principio, en su comunicación “A comprehensive approach on personal data protection in the European Union”, como the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes, entendido



como el derecho de las personas a que sus datos dejen de ser tratados y sean eliminados cuando ya no sean necesarios para los fines legítimos para los que fueron recabados.

Otros autores lo definen como el derecho a que los buscadores no localicen tus datos personales en la red. A la vista de la Sentencia del TJUE de 13 de mayo de 2014, dictada en el caso C-131/12, y siguiendo bajo el prisma de la protección de datos personales, en todo caso, tendría que definirse como el derecho que tiene un individuo a que los gestores de motores de búsqueda en Internet cesen en el tratamiento que de sus datos personales realicen en el territorio de la Unión Europea al enlazar a y al mostrar determinado contenido relativo a su persona, debido a que, habida cuenta de las circunstancias del caso en particular, dicho tratamiento ha dejado de ser legítimo, con independencia de que el tratamiento en origen continúe siendo lícito, porque, en relación con la finalidad que justificaba el tratamiento y con el tiempo transcurrido, los datos ya no son adecuados y/o pertinentes, y ahora son excesivos.

Debe entenderse, del mismo modo que se viene haciendo con el derecho de cancelación de los datos personales, que podríamos hablar de un derecho al olvido desde el prisma del derecho al honor, la intimidad personal y familiar y la propia imagen, o en relación con la propiedad intelectual (concretamente el derecho del autor a retirar su obra del comercio por cambio de sus convicciones morales o intelectuales). En tal caso, eso que se ha dado en llamar derecho al olvido podría llegar a alegarse también de las personas jurídicas en ámbitos diferentes a los de la privacidad.

El derecho al olvido debería actual en un primer tipo de supuestos serían aquellos en los que, siendo, en el origen, cierta la información que se revela respecto a un individuo, éste debe soportar esa intromisión en su intimidad por estar legitimada en virtud del derecho de información (ya sea éste ejercido a través de los medios de comunicación, ya de boletines oficiales o tablones edictales), pero en los que, debido al transcurso del tiempo, puede decirse que tal legitimación debe caducar a fin de que el individuo no tenga que soportar dicha carga durante el resto de su vida impidiéndole su propio pasado, en mayor o menor medida, vivir en paz un presente enmendado.

En segundo termino, aquellos en los que, aun siendo incierto lo manifestado respecto a una persona y viendo ésta, así, mancillado su honor, el perjudicado prefiere no actuar contra dicho ataque porque en ese momento éste no ha trascendido lo suficiente como para no poder soportar sus efectos y, sin embargo, un tiempo después, pasados ya los plazos para ejercitar cualquier acción, es recuperada esa falsa información alcanzando, en esta ocasión, mucha mayor repercusión gracias al estado de la tecnología.



A la hora de tomar decisiones, las personas lo hacemos en función de las circunstancias que entonces nos rodean y sopesando las consecuencias que nos cabe esperar con lo que conocemos en ese momento.

Teniendo en cuenta que hay determinadas circunstancias en que, ni acudiendo al derecho a la intimidad, o al derecho al honor, o al de protección de datos personales, podemos dar una solución a quien ahora se ve perjudicado por hechos sucedidos en su vida pasada, que ya habían sido olvidados por la colectividad que en su momento supo de ellos, que ahora son traídos al presente, incluso puede que con mayor virulencia que en su origen, sin que exista una necesidad que así lo justifique, provocando que dicha persona no pueda disfrutar en paz de la vida digna que ahora lleva.

El derecho al olvido debe garantizar el desarrollo de la persona acorde a lo que cabe esperar dentro del modo en que ésta dirige su vida en la actualidad, evitando que cualquier pasado, más o menos oscuro, pueda frustrar dicho desarrollo cuando no existe ya necesidad ni justificación alguna para que tenga que continuar soportando tal carga. En el entorno digital, por tanto, el derecho al olvido adquiriría una gran relevancia como medio de protección de la identidad digital o del libre desarrollo de la persona en dicho entorno, pero, sin duda, también trascendiendo de éste.

Debe tenerse en cuenta que el derecho a la intimidad a la privacidad y al derecho al honor deben ser derechos erga omnes, cuya protección debe ir más allá de las fronteras de los Estados, su garantía (recogida en la mayoría de constituciones) debe quedar salvaguarda con independencia del lugar de nacimiento o donde se encuentre el ciudadano, debe contemplarse que, de no ser así nos encontraríamos con diferentes clases de ciudadanos y derechos de diversas generaciones.

Sólo mediante el compromiso de los Estados y órganos jurisdiccionales, mediante la unificación de criterios normativos y jurisprudenciales, de tipos penales, sanciones y definición del bien jurídico protegido, puede garantizarse una correcta protección de la privacidad en la red.

Por ello, con independencia de las partes intervinientes, responsable del fichero, tratamiento, buscador, las diferentes entidades se deben dotar de medios materiales y organizativos que garanticen el correcto ejercicio de derechos por los ciudadanos, la efectiva retirada de contenidos y una información clara y concisa, entendibles por todos.

La educación debe ser un factor clave en la protección de la identidad digital de las personas, quienes en primer término son responsables de su propia información, de aquella que comparten en Internet y en las redes sociales, de sus opiniones o comentarios. Sólo desde una formación en el uso de las nuevas tecnologías y en las repercusiones que tiene compartir en la red, se puede llegar a un



sistema efectivo, junto con las garantías de ordenamientos comunes y mecanismos para la protección de los derechos fundamentales de las personas.

Es obligación de cada uno cuidar que imagen se genera en Internet, en el entendido de que es por nuestra identidad digital que se gana presencia en la esfera laboral. Somos libros abiertos para las empresas, para los clientes, y nuestra información personal ahora se puede visualizar tal como se visualiza un curriculum vitae, pues ahora existen redes sociales para concretar relaciones laborales. Son los jóvenes los que mas deben concienciarse sobre las consecuencias futuras de sus acciones presentes y a nosotros nos toca formarlos y concienciarlos para que así ocurra.