IDENTIDAD VIRTUAL: IMPLICANCIAS EN EL DERECHO A LA INTIMIDAD

Dra. Ana Karin Chávez Valdivia*

Tal vez la intimidad puede precisarse más que como un derecho como una libertad proyectada en la facultad de una persona para disponer de un ámbito de inmunidad para sus acciones privadas que permita sustraerlas de la injerencia del Estado y de terceros. De ser así, en concordancia con la identidad que es un derecho personalísimo y permite un reconocimiento en singularidad, la persona podrá construir una identidad que le es propia y solo a ella le concierne.

El desarrollo tecnológico ha convertido esta identidad en un concepto dinámico, perdiendo en cierta forma su tradicional carácter único e inequívoco y generando cuestionamientos en torno a la clásica conceptualización de la intimidad.

Por otro lado, el anonimato en Internet en nuestro país permite desvincular, desdoblar o tergiversar la identidad eliminando la responsabilidad y facilitando el actuar en un universo de identidades en el cual, mientras algunos buscan

* Doctora en Derecho y Magister en Derecho de la Empresa por la Universidad Católica de Santa María. Especialista en Derecho Informático y Gobierno Electrónico por la Universidad Inca Garcilazo de la Vega. Abogada. Conciliadora Extrajudicial. Docente asociada a la Carrera de Derecho de la Universidad La Salle de Arequipa-Perú.

achavez@ulasalle.edu.pe

protegerlas otros están interesados en descubrirlas para sus propios intereses y existe además un tercer grupo que las crea y re-crea a satisfacción personal.

INTRODUCCION

Son las 10:00 horas de un día cualquiera, en cualquier lugar del mundo, desde la comodidad de casa nos conectamos a una red social de Internet, vemos que "X" ha viajado fuera del país por vacaciones y que "Z" se ha casado, nos enteramos que "Y" va a organizar una fiesta y estamos invitados y que hemos sido etiquetados en una foto de cuando terminamos la universidad. Que "B" ha terminado con su novio y "A" perdió su trabajo. Tenemos 1001 amigos que se enteran de lo que nos pasa, lo que hacemos, pensamos, de cómo nos sentimos, etc. En conclusión, podemos tener una vida social más activa y atractiva a través de la red que en la propia realidad, sin embargo no estamos siendo conscientes que esta "interactividad social" va más allá de sólo premisas y que individualmente el brindar tanta información personal podría suponer algunos riesgos.

Hace años demandábamos la protección de nuestros datos personales sin embargo y contradictoriamente ahora los colgamos gratuitamente en la red a

disposición de cualquiera, arriesgándonos a que parte de nuestra intimidad quede a merced de los demás. Precisamente las críticas más frecuentes hacia las redes sociales en Internet se centran -al margen de su necesidad/utilidad- en su mejorable funcionalidad, masiva proliferación, en la forma como estos servicios recopilan información personal y como la utilizan, pero sobre todo en que pueden convertirse en una amenaza a la intimidad debido a que nos exigen un gran número de datos que quedan en manos extrañas y en muchos casos se debe aceptar algunas condiciones que podrían dejarnos totalmente expuestos e indefensos.

Son los usuarios de la red, en general, y de las herramientas de software, en particular, quienes deberían saber administrar muy bien la información que revelan sobre sí mismos (imágenes, datos de contactos, cuentas de correo, preferencias personales, orientación sexual, ideología, etc.) pero al no configurarse este supuesto y hacer pública la vida privada y subsecuente intimidad, pasamos del espacio personal al espacio social y desde allí al mercado. Hemos ido de la red de redes en la que participar requería de ciertos conocimientos técnicos a entornos web en los que cualquiera con un mínimo de aprendizaje puede publicar cualquier información.

Las posibilidades que ofrece la llamada web 2.0 son infinitas. Podemos afirmar que ha nacido una sociedad que se desarrolla íntegramente en el mundo virtual. En ella los individuos interactúan siguiendo en muchas ocasiones normas y pautas de conducta perfectamente homologables con las que se

producen en el mundo físico; sin embargo en muchas otras se perfilan nuevos escenarios sociales.

El nuevo entorno tecnológico obliga a reflexionar profundamente sobre hasta qué punto el derecho que regula nuestras sociedades es eficaz en el universo de las redes sociales y en este contexto constituye una cuestión fundamental establecer las reglas que deben regir respecto al levantamiento y uso de la información personal. Nos preguntamos si realmente los individuos conocen el valor de la información que proporcionan cuando se registran a un servicio, cuando navegan por internet o cuando comparten opiniones, sentimientos o fotografías en una red social. Por otro lado se debe tener presente que un significativo número de conductas patológicas que se dan en internet tienen como origen o finalidad el tratamiento de los datos personales.

Recordemos que existe una frase muy ilustrativa que dice: Nadie es tan lindo como la foto de su perfil, ni tal inteligente como sus tweets, ni tan feo como en la foto del DNI.

1.- LAS REDES SOCIALES ON LINE

Las primeras redes sociales hicieron su aparición a finales de los años 90, fueron consolidándose entre 1997 y 2001 (incorporando una serie de herramientas de uso comunitario junto a los listados de los miembros del

grupo) y se consagraron a partir del año 2002. Friendster hizo su aparición en el 2002 y Myspace en el 2003. Facebook inicia su actividad en el 2004 originalmente como una red social sólo para estudiantes de Harvard[104].

Poco a poco Facebook empezó a abrirse a otras universidades y a principios de Septiembre del 2005 se expandió para incluir profesionales dentro de redes corporativas hasta que finalmente a partir del 2006 se abrió a todo el mundo[105]. Las redes sociales se expanden y alcanzan popularidad de forma no homogénea, creciendo en determinadas áreas y países y en otros no.

Estas redes se pueden definir como aquellos servicios de la sociedad de la información[106] que ofrecen a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales facilitando la creación de redes en base a criterios comunes y permitiendo la conexión con otros usuarios y su interacción. Las vinculaciones se miden en grados donde el primer grado serían los contactos directos, el segundo los contactos de los contactos y así sucesivamente de forma que a mayor número de usuarios mayor número de vinculaciones y mayor es la red. Esta criterio puede fundamentarse en la teoría de los 6 grados de separación, es decir, en

[104] Para formar parte de dicha red era preciso disponer de una dirección de correo electrónico hardvard.edu. Esta red social fue diseñada por Mark Zuckerberg un estudiante de Harvard para hacer las veces de directorio telefónico de su facultad. Nació ligado a la metáfora: los "facebook" (libros de caras) que eran publicaciones que se repartían en los colleges americanos, una especie de anuario donde se recogían las fotos y nombres de los alumnos de una promoción.

[105] Véase: boyd,d.m.,& Ellison N.B. (2007). "Social Network Sites:Definition, history, and scholarchip". Journal of computer-mediated Communication, 13 (1), article 11.

[106] Artículo 1, apdo 2. De la Directiva 98/34/CE del Parlamento Europeo y del Consejo por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información, modificado por la Directiva 98/48/CE.

la idea de que el número de conocidos crece exponencialmente con el número de enlaces en la cadena pudiendo cualquier individuo estar conectado con cualquier persona a través de una cadena de no más de 6 grados[107]

Las redes sociales on line son un ejemplo más de la web 2.0 o web colaborativa, en la que internet deja de ser un foco de información para convertirse en un espacio virtual retroalimentado en el que los internautas consumen pero también aportan información. El usuario por tanto asume un doble papel el de consumidor y el de creador, el de interesado y responsable, ya no es más un sujeto pasivo, muy por el contrario es quien difunde información en los blogs, opina en los foros, cuelga con o sin permiso fotografías o grabaciones de videos en los que identifica amigos o conocidos sin percatarse que podrían afectar los derechos de terceros que algunas veces ni siquiera son usuarios de una red social. De esta manera son los propios internautas los que crean una gran base de datos cualitativos y cuantitativos, propios y ajenos con información relativa a la edad, sexo, localización, intereses u otros. A esto se suma el hecho de que el acceso a las redes sociales se amplía más con la aparición de nuevos medios de acceso a internet como los smartphones que además de permitir la conexión en cualquier momento, lo hacen en cualquier lugar, lo que ha provocado la proliferación de redes que facilitan la

[107] Teoría propuesta en 1929 por el escrito húngaron Frigyes Karinthy y recogida también en el libro "Six degree: The science of a connected age" del sociólogo Duncan Watts.

localización. Estos servicios que son la evolución natural de las redes sociales, apuntan además riesgos adicionales para la intimidad[108].

En esta "sociedad en red" existen servicios de redes sociales de todos los tipos y son utilizados por diversas generaciones para diferentes finalidades. Estas redes se utilizan como una forma de comunicación, expresión o "branding personal"[109] entre los usuarios y como una herramienta de marketing por parte de las empresas que cada vez más se acercan a potenciales clientes por estos medios. Aunque vivimos en un proceso de diversificación constante, podemos hacer una clasificación en al menos tres grandes grupos que cuentan con características comunes y elementos particulares que las diferencian:

1.1.- Redes sociales de comunicación

Entre otros facebook y myspace. En este tipo de plataformas los usuarios pueden registrarse en el servicio libremente mediante

---

[108] Debe señalarse que los intentos por definir a la palabra intimidad han sido innumerables. Ello demuestra de alguna manera lo dificultoso que resulta dar un concepto acabado de ese término. Quizás una de las razones de tal dificultad radique en la diferente terminología utilizada en el país en que se trate. Así, los italianos hablan de la *"riservatezza" (reserva)*, los franceses prefieren decir *"vie privée" (vida privada)* y los países anglosajones utilizan la palabra *"privacy"* (privacidad). A pesar de las distintas maneras de hacer referencia a un mismo tema, debe advertirse que todas estas denominaciones encierran un mismo sentido negativo, de exclusión, de esfera propia donde los demás no tienen cabida. Podría decirse que en principio no resulta extraño emplear los términos intimidad y privacidad como sinónimos. Hay sin embargo, quienes sostienen que ambas palabras denotan conceptos distintos. Carlos Nino en su obra "Fundamentos de derecho constitucional. Análisis filosófico, jurídico y politológico de la práctica constitucional" afirma que existe una confusión conceptual entre el bien de la intimidad y aquél que se refiere a la privacidad. Mientras la *privacidad* se conceptúa como el derecho a "ser dejado solo", como sostenía el juez Cooley en su obra de 1873 "*The elements of torts*", o el derecho de "ejercer autonomía sobre cuestiones personales significativas" -como argüía el juez Brennan de la Corte Suprema de los Estados Unidos de América-. El derecho a la *intimidad*, es definido como aquel en el cual los demás no tengan información no documentada sobre hechos, respecto de una persona que ésta no quiera que sean ampliamente conocidos. La exclusión de la información documentada se refiere a aquella que es accesible al público en general, aunque haya pasado inadvertida, dado que está registrada en publicaciones, ficheros, etc., a los que cualquiera puede acceder (no, por cierto, cuando la registración se haya hecho por un propósito muy especial y a la que haya acceso restringido)". Así, en los términos utilizados por Nino, es dable señalar que la idea de privacidad implica la posibilidad irrestricta de realizar acciones "privadas, o sea acciones que no dañan a terceros y que, por lo tanto, no son objeto de calificación por parte de una moral pública como la que el derecho debe imponer; ellas son acciones que, en todo caso, infringen una moral personal o "privada" que evalúa la calidad del carácter o de la vida del agente, y son, por tanto, acciones privadas por más que se realicen a la luz del día y con amplio conocimiento público (...)". En cuanto al concepto de intimidad, lo define el autor citado como la "esfera de la persona que está exenta del conocimiento generalizado por parte de los demás".

[109] Puede definirse "personal branding" o "marca personal" como la construcción de una imagen de la persona clara, identificable y diferenciada de los demás.

invitación y encontrar conocidos e invitarles a formar parte de su comunidad. Además estas redes proponen la vinculación con contactos de segundo o tercer grado o gente que pertenece a los mismos grupos que el usuario (colegio, universidad). En estas redes sociales los usuarios pueden publicar sus fotografías, videos, reflexiones, aflicciones y preferencias de todo tipo. Desde sus películas favoritas, hasta la religión que profesan o la orientación política o sexual.

1.2.- Redes sociales especializadas

Este tipo de redes sociales se centran en un eje temático con la finalidad de unir a colectivos con los mismos intereses (fotografía, viajes). Algunos ejemplos podemos verlos en las redes como flickr.com para compartir fotos, virtualtourist.com para viajeros, redes sociales de microblogging[110] como twitteer.com; entre otros.

1.3.- Redes sociales profesionales

Pueden clasificarse como una categoría propia (linkedIn.com) y permiten a los individuos de todo el mundo buscar nuevas oportunidades de empleo, hacer "networking" con compañeros de trabajo, con gente con la que han intercambiado una tarjeta, con profesionales del sector mediante contactos comunes de confianza.

[110] El microblogging permite a los usuarios enviar y publicar mensajes breves generalmente de solo texto mediante sitios web, a través de SMS, mensajería instantánea o aplicación para móviles.

2.- FUNCIONAMIENTO DE LAS PLATAFORMAS DE REDES

En términos generales y sin atender a un modelo concreto de red social, el funcionamiento se estructura en tres fases: registro, utilización y baja en la red social. Debe tenerse presente que participar en una red social entraña una serie de riesgos que pueden surgir en diferentes momentos.

2.1.- Momento de registro. Pude hacerse motu propio o por invitación y suelen solicitarse los datos básicos (nombre y apellidos, dirección de correo electrónico, sexo y edad). Por la finalidad de esto servicios, es habitual que las redes sociales sugieran al usuario importar los contactos de su cuenta de correo, para lo que éste tiene que dar el consentimiento mediante la introducción de su contraseña, permitiendo invitar a aquellos que todavía no forman parte de la red. Es en este momento cuando al usuario suele guiársele para la configuración de sus opciones de privacidad. Los riesgos específicos relativos a esta fase son los relacionados con la falta de una correcta información, la seguridad de los datos y la configuración de sus opciones de privacidad[111].

[111] Los proveedores de estas redes tienen que adoptar las medidas técnicas y organizativas necesarias para mantener la seguridad e impedir accesos no autorizados, implantando por defecto opciones de privacidad protectoras ya que la gran mayoría de los usuarios no realizarían cambios en el futuro en esa configuración.

2.2.- Utilización se la red social. El usuario desarrolla su actividad en la red actualizando su estado e interactuando con los otros usuarios. Al utilizarla, los usuarios van creando un perfil con datos relativos a intereses, estudios, localización, hasta la ideología. Además, con la utilización y publicación de información, pueden difundirse en el perfil datos de otras personas. Las principales plataformas de redes sociales están configuradas en tres niveles de privacidad (amigos-primer grado de relación-, amigos de amigos –segundo grado- yoda la red- con todos los miembros de la red independientemente de su relación). De esta manera, según confiere el usuario su privacidad, la información podrá tener distinto alcance.

Entre otros servicios que puede ofrecer la red social se encuentran el servicio de chat, buzón para mensajes de texto, espacio para publicar fotos, grupos de noticias, foros de discusión, blogs, eventos, geolocalización y buscador mediante el que se puede localizar a otros miembros de la misma red, empleando diferentes criterios de búsqueda. Todos ellos se sirven de cookies para personalizar el sistema y también la publicidad. En esta fase las preocupaciones se centran en el desconocimiento del alcance de la información publicada por el usuario, su posible utilización para otras finalidades, el tratamiento de datos de terceros o la suplantación de identidad.

2.3.- La baja de estos servicios o cancelación de la cuenta. Conlleva entre sus riesgos específicos la dificultad para eliminar de manera real y

efectiva la cuenta de usuario, puede provocar que la información continúe disponible sin su conocimiento[112].

Si bien las amenazas referidas son importantes existen autores que ponen de relieve otros peligros que quizá siendo menos evidentes tienen mayor trascendencia. Este es el caso de Dumortier que considera que el mayor riesgo de las redes sociales es la descontextualización de la información, de los datos que aparecen publicados[113]. Este autor sigue la terminología acuñada por Nissenbaum quien considera que se produce descontextualización de la información o de los comportamientos cuando éstos son utilizados en un contexto distinto de aquel para el cual se emitieron[114].

En el caso de Facebook probablemente se acentúen estos riesgos debido a algunas características inherentes a dicha red social tales como la dinámica de simplificación que entraña, la diseminación de una gran cantidad de información y finalmente el efecto globalizador que implica que sin estar en Facebook, el sujeto puede ser objeto de Facebook, de tal forma que la persona se convierte antes en objeto de una red (se cuelga una foto identificándola con el nombre) que en sujeto de una red. Además se da la circunstancia de que

[112] El GT29 (Grupo de Trabajo que reúne a las autoridades de protección de datos de los 27 estados miembros donde el Supervisor Europeo de Protección de Datos y la Comisión -que actúa como secretario creado por el artículo 29 de la directiva 95/46/CE- cuentan con carácter consultivo e independiente para la protección de datos y el derecho a la intimidad) recomienda que si un usuario no actualiza el servicio durante un periodo definido de tiempo, el perfil deberá desactivarse . Transcurrido además otro periodo de tiempo el perfil deberá ser borrado.
[113] Véase Http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_esp
[114] Véase Http://www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf

para poder ejercer los derechos de rectificación o cancelación es preciso estar registrado en dicha red.

3.- LA IDENTIDAD EN LA RED

Bajo la expresión “identidad digital” o “identidad virtual” se han venido agrupando de forma reciente las técnicas que permiten a las personas y a las organizaciones identificarse y actuar en las redes, mediante mecanismos de autenticación de mayor o menor robustez.

En una concepción muy simple se entendería esta identidad como el conjunto de datos (a menudo denominados “atributos”) que nos diferencian suficientemente del resto de personas o entidades, en un ámbito concreto, como por ejemplo el nombre y apellido, el nombre de los padres, los códigos de identificación que se nos asignan y otros, en el caso de las máquinas la dirección IP o el nombre de dominio en internet y otras redes.

Ignacio Alamillo Domingo denomina a la identidad en la red como “identidad electrónica”, distinguiéndolas según el uso habitual por las personas en las siguientes clases:

a) *Identidad electrónica “personal”* aquella que nos identifica de forma autónoma, sin conexión con organización alguna. Se trata de una identidad legalmente regulada por el estado, válida dentro de su territorio, especialmente basada en procesos robustos de identificación física. En algunos países se acredita con el DNI electrónico.

b) *Identidad electrónica “corporativa”* aquella que nos vincula con una organización pública o privada mediante una relación jurídica de pertenencia o vinculación y frecuentemente se construye sobre el documento de acreditación de la identidad física personal como sucede con el fotocheck de un trabajador o funcionario, un carnet de profesional colegiado u otros. Se trata de una identificación obligatoria dentro de la corporación empresa, justificada por la relación laboral o afín.

c) *La identidad electrónica del “cliente”* aquella que nos vincula con una organización pública o privada con la que se establece una relación de negocio con vocación de permanencia, como sucede con la identidad financiera, programas de fidelización, entre otros. Se trata de una identificación obligatoria en algunos casos debido a requisitos

regulatorios (como en el caso de la identificación financiera) y voluntaria en el resto de casos con el objeto de ofrecer al cliente servicios más personalizados, descuentos, regalos u otras compensaciones en caso de un determinado volumen de consumo.

Señala asimismo Alamillo, que todas estas identidades que nos son "suministradas" o atribuidas por "proveedores" o personas diferentes a nosotros mismos, son electrónicas, porque se asignan, almacenan y gestionan por medios electrónicos, en bases de datos de identidad que varían desde silos de identidad completamente desconectados entre sí hasta complejas redes de identidad interconectada en los dominios financieros o de lucha contra la delincuencia.

Si bien esta clasificación es bastante certera, sobre todo en aquellos países que emplean el DNI electrónico, creemos que para el entorno de las redes sociales de comunicación no serían los más precisos, a pesar de que los medios electrónicos juegan un papel preponderante. Además todas estas identidades son denominadas "identidades de segunda o tercera parte" porque nos son suministradas por organizaciones o personas diferentes a nosotros[115].

[115] Son identidades de segunda parte cuando sólo sirven para relacionarnos con la organización o personas diferentes a las que nos la ha suministrado, como sucede con las identidades acreditadas mediante certificados reconocidos de firma electrónica, regulados por ley.

Consideramos que la identidad virtual propiamente dicha es aquella que sin estar necesariamente vinculada con alguna institución u organismo (como sería la identidad electrónica corporativa o de cliente) y que además sin necesidad de contar con el respaldo del estado (el caso de la identidad electrónica personal) es creada en la red como un tipo de identidad parcial[116], convirtiéndose en un nuevo paradigma en la gestión de la identidad debido a que se basa en una gestión realizada únicamente por el propio usuario de todo el ciclo de vida de su identidad, con mayor control sobre la divulgación de sus datos personales.

Podemos afirmar que una de las principales diferencias entre una identidad electrónica y una virtual se centran principalmente en la existencia de cierta clase de "autenticación" respaldada por determinados organismos o instituciones que garantizan y corroboran la vinculación entre la persona física de existencia real y la que se halla en la red.

Son precisamente estas identidades denominadas "de primera parte"[117] que prometen un nuevo modelo de privacidad bajo un verdadero control del usuario. Una identidad en la cual y en muchos casos podría no existir la menor

[116] El término identidad parcial hace alusión a un subtipo de identidad que sirva para identificar a un individuo en diferentes contextos o roles. Por ejemplo parece coherente que un individuo concreto pueda ser titular de diversas identidades que acrediten su rol como trabajador, cliente de una entidad bancaria, administado tributario que le permitan actuar en diferentes contextos. Y de hecho parece también coherente que para obtener cada uno de esos diversos tipo de identificación no sea necesario aportar el mismo grado de información ya que, en caso contrario, se estaría vulnerando el principio de proporcionalidad.

[117] Que a diferencia de las identidades electrónicas personales no están reguladas por el estado y mucho menos basadas en sólidos procesos de identificación física.

coincidencia entre la persona física real e identificable y la identidad virtual asumida.

Todos, en cierta forma, tenemos muchas identidades parciales, adecuadas a los diferentes roles o actividades que realizamos durante nuestra vida, cuyo uso está protegido de manera particularmente intensa por las leyes de protección de los datos de carácter personal.

Sucede que en la red -a diferencia de lo que dice la intuición en el mundo físico- vamos a disponer de forma natural (y debido a la presión legal de la privacidad según el contexto) de diversas y variadas identidades, en algunos casos con sus correspondientes mecanismos de autenticación y en otros no. Es decir, en las redes sociales no es posible contar con una identidad única y mucho menos garantizarla. Este panorama nos hace replantearnos la necesidad de abrir el debate en torno a la conveniencia o capacidad legal de crear y asignar códigos de identificación universal que garantizara la existencia de un entorno tecnológico organizado y jurídico compartiendo la identidad y autenticación de los usuarios entre varios sistemas basados además en normas de confianza mutua y un código de ética.

4.- RESPONSABILIDAD DE LOS ACTORES IMPLICADOS EN LAS REDES SOCIALES Y LA NORMATIVA APLICABLE

En el entorno de las redes sociales existen diversos agentes implicados; el propio proveedor de servicios de redes sociales, los usuarios, los creadores de aplicaciones que se integran como servicios adicionales en la plataforma. Además también podríamos incluir a los anunciantes de estas redes sociales en el proceso, en aquellos casos en los que la red social facilite información sobre los usuarios de los mismos.

Por su importancia para este trabajo nos referiremos solo a los dos primeros:

a) *Los proveedores de servicios de redes sociales* son responsables cuando tratan datos para su propia gestión, debiendo cumplir en su caso con las obligaciones derivadas. Son ellos los que tratan los datos de los usuarios para el registro y cancelación de la cuenta y proporcionan mediante el diseño de su plataforma los medios que permiten el tratamiento de la información y la interacción entre los usuarios. Además utilizan estos datos para finalidades publicitarias, realizando tratamientos sobre los mismos con el fin de ofrecer un target al anunciante.

En algunas redes sociales la plataforma permite que desarrolladores externos creen aplicaciones (juegos, cuestionarios, etc.) que tratan datos de los usuarios. Los proveedores de aplicaciones también pueden ser responsables del tratamiento si acceden a la información de los usuarios.

b) *Los propios usuarios*, que pueden ser personas físicas o jurídicas, también forman parte del proceso. Es aquí donde se encuentra la particularidad de este tipo de servicios. Si bien, las personas suelen ser, "afectados o interesados" en otras ocasiones estas toman las decisiones sobre la información que tratan, pudiendo llegar a ser considerados como responsables del tratamiento y asumiendo las obligaciones a los que éstos están sujetos teniendo además que prestar un deber de diligencia.

Tal como hemos señalado existen diversos actores involucrados y por tanto con cierto grado de responsabilidad, sin embargo, debe tenerse presente que la atribución de responsabilidades demanda una normativa previa que establezca aquellas conductas susceptibles de tutela o de sanción y las consecuentes responsabilidades para los actores dentro del ámbito que nos ocupa, y es precisamente en éste donde nuestro país carece de regulación.

Nuestra legislación en materia de protección de datos personales tanto Ley Nro. 29773 del año 2012 y su correspondiente reglamento el Decreto Supremo Nro. 003-2013-JUS excluye de su ámbito de aplicación aquellos tratamientos que realicen las personas "en el ejercicio de actividades exclusivamente personales o domésticas". Más aún, expresamente limita la protección de datos al territorio peruano.

En este sentido, precisa en su artículo 3° inciso 1 que la ley se aplica a los datos contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realice en el territorio nacional, siendo objeto de especial protección los datos sensibles. Continúa la norma señalando que las disposiciones de la ley no son de aplicación a los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales creados por personas naturales para fines exclusivamente relacionados a su vida privada o familiar. El reglamento ratifica ésta limitada protección al reiterar en su artículo 4° que sus disposiciones no serán de aplicación al tratamiento de datos personales realizado por personas naturales para fines exclusivamente domésticos, personales o relacionados con su vida privada o familiar.

Sin embargo, nuestra norma no contempla la posibilidad de que en algunas situaciones el tratamiento por parte de los usuarios de las redes sociales podría exceder la actividad doméstica. El hecho en mención si ha sido considerado por la comunidad europea a través del GT29 y considera las siguientes situaciones:

- La primera de ellas, cuando la red social se utiliza como una plataforma de colaboración para una asociación o una empresa “con fines comerciales, políticos o sociales”
- Asimismo, otro de los indicativos de que se está excediendo del ámbito doméstico, es cuando manifiestamente el usuario tenga más contactos

de los que bajo un criterio de racionalidad podría considerarse como contactos reales. En estas situaciones que habrían que analizarse caso por caso, puede llegar a ser considerado como un responsable del tratamiento.

- Existe un tercer caso particularmente importante en que el usuario puede considerarse responsable del tratamiento y es aquel en cual al tratar datos de terceros se vulneren sus derechos. Es decir la exclusión de la actividad doméstica se ve también limitada por la necesidad de garantizar los derechos y especialmente lo referente a los datos sensibles. En este sentido se estarían dando también nuevas situaciones como “menores responsables”.

Si recogiéramos estos criterios en nuestra legislación la regla general sería que salvo estas excepciones, que deberían aplicarse con prudencia, las actividades que lleve a cabo un usuario, dentro de una red social y que no sean objeto del ámbito de aplicación de la Ley de Protección de Datos podrían ser objeto de otras leyes como aquellas de protección al derecho al honor, a la intimidad personal e imagen o por disposiciones generales del derecho civil o penal según sea el caso.

Sin embargo, en cuanto al segundo indicador señalado, tendríamos la tarea de precisar de manera puntual cual sería el criterio de racionalidad y su correspondiente sustento para poder determinar en qué momento se considera que un sujeto tiene demasiados amigos.

En lo referente al tercer aspecto, tendríamos que determinar hasta qué punto los usuarios de las redes sociales son considerados responsables del tratamiento cuando publican información de terceras personas, esto, no sólo a efecto de saber en qué momento empiezan a ser considerados "responsables menores" y establecer la correspondiente sanción en relación a este grado sino también para determinar que tan sensibles serían los datos con los que estamos tratando o si tal vez las redes sociales han llegado a "desnaturalizarlos".

De acuerdo a nuestra ley de protección de datos personales los datos sensibles están constituidos por datos biométricos, datos referidos al origen racial y étnico, ingresos económicos, opiniones y convicciones políticas, religiosas, filosóficas o morales. Afiliación sindical, e información relacionada a la salud o la vida sexual. El reglamento de la ley recoge los mencionados anteriormente con excepción de los datos biométricos y precisa información referida a la salud catalogándola como física o mental u análoga; así mismo menciona como datos sensibles hechos o circunstancias de la vida afectiva o personal y hábitos personales que corresponden a la esfera más íntima de la persona.

En consecuencia, saldríamos de la esfera de la actividad doméstica con el tratamiento de los datos sensibles de terceros, pero como señalamos nuestra legislación presenta como datos sensibles muchos de aquellos que son

compartidos libremente en las redes sociales perdiendo su naturaleza de “sensibles”. Por tanto, difícilmente se configuraría una exclusión de actividad doméstica y una responsabilidad menor, dado que contradictoriamente gran cantidad de lo que es considerado información sensible en nuestro país según la ley, es una información solicitada por las mismas redes sociales y es una información que el usuario brinda de manera voluntaria y en consecuencia con un consentimiento implícito.

Debemos tener presente que muchas veces la actuación de los usuarios en el ámbito de las redes sociales se encuentra abocada a provocar conflictos de derechos al menos en lo que se refiere al derecho a la información, la libertad de expresión y el derecho a la protección de datos.

Más aún, el conjunto de riegos que hemos mencionado precisa una mayor atención cuando nos referimos a los menores llamados “nativos digitales” que no habiendo alcanzado un grado de madurez suficiente, se han incorpora do con fuerza a las redes sociales. En entornos virtuales los menores actúan con amigos en tiempo real, crean, se unen a comunidades de su interés, (música, deporte) se comunican mediante blogs o mensajes instantáneos, hacen nuevos amigos, comparten imágenes, videos, música y experimentan su propia identidad en nuevos espacios como las redes sociales. Este colectivo,

que ha nacido con la tecnología ya plenamente arraigada tiene otro concepto de la intimidad[118].

Se desprende que las redes sociales y en general la Web 2.0 constituye un fenómeno con características peculiares dentro de Internet, que ya es en sí un ámbito singular para el derecho[119]. Estas redes suponen un tipo de comunicación muy peculiar. Si el estatus jurídico de una comunicación depende fundamentalmente de su carácter público o privado, las comunicaciones sociales se sitúan, cuando menos en una zona gris. Esta incertidumbre enlaza con otra no menos trascendente. Desde un punto de vista jurídico no está claro si los datos que los usuarios ponen en poder de las redes sociales, son datos que pertenecen a una comunicación entre privados que tienen lugar de manera continuada y por tanto está protegida por el secreto de las comunicaciones o si en cambio deben ser considerados meros datos almacenados, suministrados voluntariamente por los usuarios, es en este supuesto donde el derecho de protección de datos resultaría aplicable.

Por si fuera poco nos encontramos además con un problema de consentimiento que puede afectar tanto a la protección del derecho al secreto de las comunicaciones, como a la protección de datos personales. La

[118] El Memorando de Montevideo adoptado en julio del 2009 en la ciudad de México sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, recoge una serie de recomendaciones dirigidas a distintos actores a fin de alcanzar una mayor protección de la privacidad de los menores de edad. Véase http://memorandumdemontevideo.ifai.org.mx/index.php/features. Si bien nuestra legislación señala puntualmente la intervención de los representantes legales para la protección de los datos personales de niños y adolescentes, no hace alusión a las redes sociales que es precisamente el ámbito donde mayor protección requerirían y esto en base a la excepción del ámbito de aplicación de la ley de datos personales señalada.

[119] Las redes sociales han inaugurado un nuevo tipo de negocio basado en la minería de datos, que ha dado luz a nuevas formas de cooperación entre el estado y el sector privado

protección del secreto de las comunicaciones y autodeterminación informativa[120] tienen en común el que son instrumentos para la protección de la intimidad. En tanto el primero es un derecho de exclusión, el segundo es un derecho de control sobre los datos.

En lo que atañe a las comunicaciones que es el supuesto que más interesa, resulta fundamental la distinción entre comunicaciones abiertas y cerradas. La participación en un foro abierto o la publicación de un artículo en una web no quedan protegidos ni por el secreto de las comunicaciones ni por la protección de datos en cuanto que aquí surge un interés constitucional prevalente como sería la libertad de expresión o el derecho de autor. Sin embargo, el problema de las redes sociales situadas en este contexto es que supone una suerte de tertium genus entre comunicaciones pública y privada, donde el usuario puede elegir además entre niveles de publicidad muy variados.

Aunque, por ejemplo, las agencias de datos europeos han manifestado que las redes sociales deben respetar las normas de privacidad de los países en los que operan, lo cierto es que esta declaración no pasa de ser un simple desidaratum, entre otras cosas porque Facebook indica en sus condiciones que la legislación aplicable en sus relaciones con sus usuarios serán las del estado de California.

[120] El Código Procesal Constitucional del Perú, Ley N° 28237 recoge en su Título cuarto la protección de este derecho y el correspondiente procedimiento de tutela a través de la acción de Habeas Data.

El usuario de redes informáticas aunque presta su consentimiento, dudosamente sabe para qué lo presta, y es también dudoso que conozca realmente las implicaciones que para su intimidad supone la participación en una red social y en general en la web 2.0. Pero aún hay más, todo este nivel de incertidumbre se combinan con un grave problema de vigencia territorial de la ley. Los sitios más usados como Facebook o Google están situados en los Estados Unidos, lo que supone un marco jurídico que parte de principios sustancialmente distintos a los europeos y a los países de habla hispana.

Además debe tenerse presente que las redes sociales on line al haber cambiado la forma en que las personas se comunican, permanecen en contacto, comparten opiniones o ideas; al haber creado otra forma a través de la cual se puede encontrar trabajo o a una pareja, podrían paralelamente producir la afectación de otros derechos además del derecho a la intimidad personal, familiar y a la propia imagen, como podrían ser el derecho al honor sin perjuicio de comprometer además el derecho la propiedad intelectual o suscitar un conflicto entre el derecho a la privacidad y el derecho a la libertad de información y expresión.

Nos encontramos entonces ante una serie de interrogantes legales respecto al tratamiento de la información personal, por lo tanto resulta fundamental determinar que repuestas ofrece el derecho ante estos fenómenos y establecer hasta qué punto facilita herramientas efectivas para regular esta

nueva realidad ya que un individuo no puede definir que es la privacidad o la protección de datos personales hasta que se encuentra con ella cara a cara.

Sin duda hablar de la sociedad de la información y de las redes sociales en Internet es hablar en cierta medida de relaciones privadas internacionales, es decir del Derecho Internacional Privado. Los posibles problemas de vulneración de datos de carácter personal derivados de la utilización de redes sociales en internet podrían ser resueltos a partir de las normas del Derecho Internacional Privado relativa a la responsabilidad civil contractual o extracontractual, sin embargo, de ser así, los problemas girarían en torno a la determinación del órgano jurisdiccional competente para conocer del litigio así como la ley aplicable para resolver el conflicto.

Tal vez una probable unificación de las normas estatales en esta área del derecho en torno a la problemática planteada sobre la protección de datos en las redes sociales podría evitar la relatividad de las soluciones y/o la utilización de criterios subjetivos, flexibles y particulares y permitir la vinculación del supuesto concreto con un país determinado.

Es de suma importancia que estas cuestiones sean abordadas por los legisladores ya que tal como señala Ricard Martinez[121] en internet, al menos

[121] Martinez Martinez, Ricard. "El derecho fundamental a la protección de datos: perspectivas" en Internet, derecho y Política. Las transformaciones del derecho y la Política en 15 artículos. Editorial UOC, Barcelona, 2009. Pp. 141-165

tal y como lo conocemos, ni existe el derecho al olvido, ni la posibilidad de garantizar que la identidad digital de cada ciudadano sea veraz y sujeta completamente a su propio control.

UNA SOLUCION APARENTE

El marco normativo en que se produce la recolección y gestión que de los datos de los usuarios hacen redes sociales en internet y los servicios 2.0 se ha desarrollado bajo la influencia de un discurso de autorregulación[122]. Considerando que en un periodo de tiempo muy corto estos servicios han pasado de no existir a tener la relevancia social que ostentan hoy el modelo de autorregulación de las empresas web 2.0 es el propio de un sector que todavía los distintos actores reguladores no han prestado plena atención. Nos encontramos por tanto ante un sistema en el que son las empresas las que ejercen un papel abrumadoramente dominante en la formación del sistema de derechos y garantías y en el que con frecuencia la autorregulación se confunde con desregulación y libertad contractual o empresarial. Son esencialmente las empresas las que regulan el funcionamiento de sus servicios.

Facebook constituye una suerte de pequeño ordenamiento jurídico con distintos instrumentos normativos internos el documento más importante, al

[122] Arroyo Jimenez y Nieto Martin (dirs.) Autorregulación y sanciones. Lex Nova. Valladolid. 2009

menos de cara al usuario es el de “Política de Privacidad”[123], pero también hay una Declaración de Derechos y Responsabilidades”[124] que rige la relación de la empresa con los usuarios y con todos aquellos que interactúan con Facebook y que tiene su origen en “Los Principios del Facebook”[125]. Estos documentos abordan temas comunes, lo que causa cierta sensación de dispersión. Adicionalmente hay muchos otros documentos lo que hace que en definitiva se convierta en un sistema de normas complejo y confuso digno casi de ser sometido a un proceso de codificación.

Una de las funciones comunes de la política de privacidad de las redes sociales en internet es la de desplazar el riesgo hacia el usuario. La política de privacidad se encargará de dejar claro que son riesgos inherentes a “compartir información” y no a las características técnicas o empresariales de su modelo de negocio así como a una actuación externa de software e individuos maliciosos y no del propio sitio. Sin embargo no necesariamente es verdad la imposibilidad técnica de controlar el flujo de información. El caso más claro es el de la publicación y etiquetado de fotografías en las que aparecen terceras personas sin su consentimiento. Facebook no ofrece al usuario la opción de impedir esta actividad. Es más ni siquiera ofrece la opción de que el etiquetado de la fotografía (que enlaza inmediatamente al perfil de la persona que aparece en ella) haya de llevar aparejado el consentimiento del “fotografiado” como ocurre por ejemplo en las solicitudes de amistad. El resultado es un

[123] Véase el sitio web donde se alojan los documentos oficiales del facebook (facebook site governance)
[124] "Declaración", "Condiciones" o "DDR"
[125] Véase https://www.facebook.com/principles.php

tedioso procedimiento de desetiquetado. Esto implicaría ignorar uno de sus principios generales sobre el consentimiento previo y debemos recordar que el consentimiento es la pieza angular a partir de la cual se construye el sistema de protección de datos personales.

DESAFIOS QUE PLANTEAN LAS REDES SOCIALES.

Por sus implicancias en la privacidad, ya en octubre del año 2007, la European Network and Information Security Agency (ENISA) publicó su documento "Security issues and recommendations for on line social networks" en el que se señalaban los principales desafíos en estas redes ofreciendo una serie de recomendaciones. Por otro lado, El International Working Group on Data Protection and Telecomunications (IWGDPT) en el que participa la Agencia Española de protección de datos (AEPD) viene haciendo un seguimiento de este tema desde que en marzo del 2008 aprobara en su cuadragésima tercera reunión celebrada en Roma, el Rome Memorandum[126]. En opinión de este grupo uno de los principales desafíos para la privacidad está en el hecho de que son los propios usuarios los que publican grandes cantidades de información y las legislaciones tradicionales están dirigidas a regular el tratamiento de datos por parte de las administraciones y empresas. Esta afirmación se verifica claramente en nuestra legislación sobre datos personales la cual establece en el artículo 1° del Reglamento la regulación del

[126] Véase Http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

adecuado tratamiento de datos tanto por las entidades públicas como por las instituciones pertenecientes al sector privado y en este sentido a través de la Resolución Directoral 001-12013-JUS/DGDP del 8 de mayo del 2013 aprobó los formularios para la inscripción de bancos de datos personales de administración privada por persona natural, de administración privada por persona jurídica y de administración pública.

Otro tema en el que este grupo pone atención es en la actividad on line de las denominados “nativos digitales” aquellos que han nacido y crecido en el entorno de la tecnología como Internet o la telefonía móvil y que teniendo otro concepto de privacidad, tal como señalamos anteriormente, se sienten cómodos publicando detalle de sus vidas en Internet. Tal vez esta sea una de las razones que nos permita replantearnos el hecho de que la intimidad se precise más que como un derecho, como una libertad proyectada en la facultad de una persona para disponer de un ámbito de inmunidad para sus acciones privadas que permita sustraerlas de la injerencia del Estado y de terceros.

Curiosamente la vida privada o la intimidad personal y el concepto tradicional que éstas encierran parecen ser algo diametralmente opuesto a la finalidad que tienen las redes sociales, donde compartir información no es sólo un requisito fundamental sino su razón de existir.