XVIII Fiadi CR

13 de Octubre

CONFIANZA Y DERECHO EN LA ERA DIGITAL

Julio Téllez Valdés
UNAM (México)

La *Confianza Digital,* es un rubro que va más allá de un tema de estudio o análisis jurídico. Se trata de un gran trabajo integrador que tiene a la confianza como una piedra angular, tomando como punto de partida el enfoque de la privacidad y la protección de datos y la "seguridad de la información", como derechos fundamentales que construyen la base para el desarrollo y mejoramiento de los sistemas jurídicos contemporáneos en materia de Tecnologías de la información y Comunicación (TIC), estrechamente vinculados con la seguridad para los entornos económicos y sociales de la información, la tecnología *per se* y la cultura digital.

Se identifica como variable principal y eje toral de ésta ponencia a la "confianza en la Era Digital", para la construcción de los grandes beneficios que pueda arrojar el uso de las TIC, tanto a nivel gobierno, empresarial o personal. Es un presupuesto básico para el crecimiento y desarrollo económico y social que se busca con la sinergia de los distintos sectores de la sociedad: público, privado y social.

Los beneficios de este enfoque de jurídico, surgen de un fenómeno social complejo como la Sociedad red y la economía digital. El uso generalizado de

las TIC –bienes y servicios tecnológicos- tiene implicaciones jurídicas evidentes donde la confianza se vuelve pieza clave.

El problema de –la falta de confianza- derivada de la ausencia de elementos: *tecnológicos, normativos y culturales*, deben ser analizados a efecto de dimensionar lo complejo del fenómeno y reducir al mismo tiempo dicha complejidad a través del análisis jurídico de dichos elementos para con ello ofrecer soluciones armónicas que aporten a los ámbitos social, cultural, económico, político y jurídico en la convivencia de los diferentes sectores de la sociedad.

El origen de esta ponencia es determinar el grado de impacto del derecho en la confianza digital, y su correlación de ésta con las principales actividades del sector público, privado y social, con la intensión de que el derecho mediante la certeza jurídica –análisis, propuestas de reformas legales, etc.,- contribuya a elevar los beneficios del uso de las TIC en la sociedad y sus diversos sectores.

El Derecho, como agente que de impacto en la Era Digital, donde la confianza –*tecnológica, jurídica y cultural- configuran un ecosistema dinámico virtuoso* para la construcción de valores que determinan la conducta del ser humano –mismas que regula el derecho-, que detona o reprime la actividad de los diversos sectores –sistemas- *de los distintos países en la Era digital*.

*D*esde el inicio de la sociedad ha sido clave para la subsistencia de sus individuos, buscar el estado de confianza, protección y seguridad. Así, la confianza está vinculada a la seguridad, tranquilidad y ello a la subsistencia

humana, con lo cual los individuos pueden hacer actividades recreativas, económicas y de gobierno. En la época contemporánea bien pude resumirse en la siguiente frase: *La confianza es la base para el desarrollo y éxito de la sociedad en la Era digital*.

Así, la confianza -clave para la interacción entre los diferentes sectores de la población– donde la interacción que en sus actividades conllevan relaciones jurídicas o actos jurídicos y por ende, se convierte en el motor del análisis sobre el cual se atenderán las carencias de confianza en la Era Digital, lo cual implica sin lugar a dudas un gran desarrollo inter y transdisciplinario.

Es un proceso complejo que se analizará desde el enfoque jurídico, considerando los siguientes componentes o temas dentro del Derecho de las TIC:

a) Tecnológico (TIC):

- Utilizando Tecnologías de mejor privacidad (PET),
- Aplicando Privacidad desde Diseño (*Privacy by Design*) en las TIC*,*
- Uso de las TIC en sector público*, de software* y aplicaciones, respecto de sus efectos en la privacidad.
- Computo en la nube
- Cibercrimen

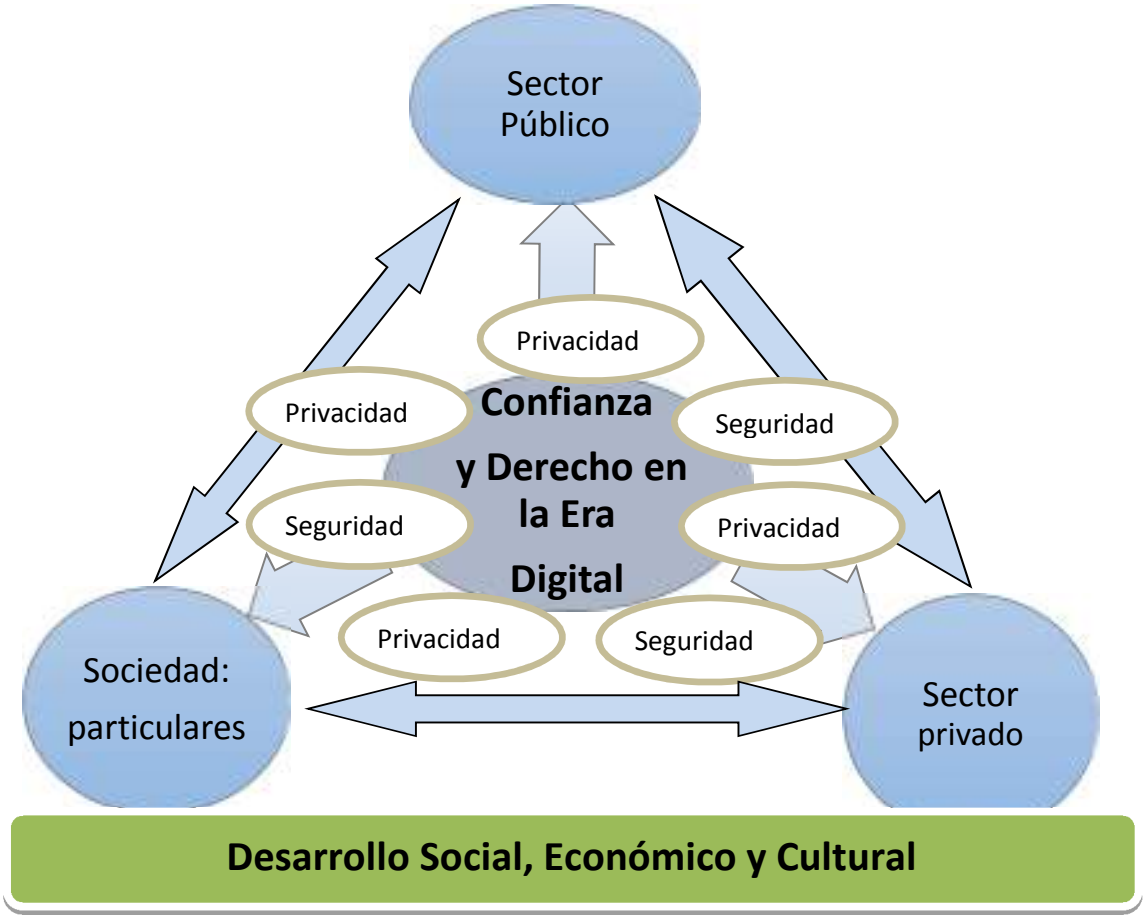
b) Derecho en la Era Digital (Marco normativo y certeza jurídica):

- Mejoramiento de normas pertinentes en materia de Derecho de las TIC, destacando el de la Privacidad, protección de datos y la seguridad de la información.
- Desarrollo de normas técnicas en relación a: privacidad, tratamiento de datos y seguridad de la información.
- Revisión del marco jurídico para su armonización y adecuación a la Era Digital y la dinámica de las TIC

c) Aspecto cultural en el uso de las TIC (cultura digital):

- Cultura de la legalidad, del respeto a los Derechos Humanos y TIC
- Cultura de la Privacidad y la protección de datos
- Cultura de la Seguridad de la información
- Capacitación y desarrollo de habilidades a los actores jurídicos

De manera gráfica, un esbozo del análisis jurídico es el siguiente:



En la interacción de los distintos sectores –sistemas- hay temas interconectados donde el principal fin; es alcanzar beneficios gracias al uso de las TIC's. Sin embargo, existe una fuerte **desconfianza** en su manejo, regulación y aplicación, sea por ignorancia u otra causa, es el principal reto para la Economía digital, para el desarrollo del gobierno digital y los procesos de innovación tecnológico de los que hablan empresarios, académicos y políticos e incluso lo son para las actividades de la vida cotidiana de la sociedad simples como el uso de redes sociales, pagos por internet, o compra de aplicaciones de ocio. Además de que no hay un marco jurídico y operadores jurídicos del todo actualizados y capacitados –existen fuertes trabas, omisiones o lagunas jurídicas, imprecisas y desafortunadas normas y malas

interpretaciones jurídicas-. Esto hace evidente la necesidad de aportar desde la ciencia jurídica; solución integral -tecnológica, jurídica y cultural-, encaminada a incrementar la *Confianza Digital:*

Tecnologías (TIC's)
+
Seguridad de la información (Si)
+
Certeza jurídica (Cj)
+
Cultura Digital (Cd)

} **Confianza Digital**

Beneficios:

Del sector privado: desarrollo económico; potencializar el sector económico, comercio electrónico, transferencias y pagos electrónicos, y creación y crecimiento de MPyME, bancarización, etc.

Del sector público: eficiencia del gobierno en la gestión pública: eficacia, transparencia, rendición de cuentas, respeto a Derechos Humanos y en el ámbito democrático la legitimidad respecto de la población (Estado eficaz: desarrollo cultural, social y económico).

Del sector social o en lo individual: la relación entre sí y los sectores público y privado, en términos cualitativos y cuantitativos económicos, de calidad de vida y de gobernabilidad. Reconocimiento de un vivir en un Estado Democrático de Derecho.

Círculo virtuoso entre las actividades económicas productivas, de gobierno y socio culturales.

Esta ponencia integra el estudio de varios temas particulares en relación a la privacidad, la protección de datos y la seguridad de la información. En esta tesitura, partimos de las siguientes consideraciones:

- La Privacidad debe entenderse como algo dinámico de corte sincrónico y al mismo tiempo longitudinal para poder ofrecer estudios jurídicos de mayor aproximación a la complejidad del sistema social; comprendiendo el sector público y privado.
- Es un valor personal subjetivo y constructo interno y colectivo determinado por circunstancias, fenómenos y agentes dinámicos como las tecnologías, la cultura y las políticas, etc. Transformándose constantemente el enfoque social, económico y jurídico desde el cual se observa.
- La Privacidad es un Derecho Fundamental que cobra mayor relevancia en esta Era digital donde el flujo y recopilación de datos es de lo más usual.
- La Protección de Datos es un derecho fundamental por separado al de Privacidad, aunque interdependiente como derecho humano y también fundamental.
- Tanto el derecho a la privacidad como el derecho a la protección de datos, se vinculan para su efectivo cumplimiento con las TIC y la seguridad de la Información, aunado a la carga cultural respecto de los tres anteriores.

- Para que se pueda generar “confianza” se requiere de un trabajo integral y constante; resaltando el enfoque jurídico capaz de comprender la necesidad del trabajo multidisciplinario y complementario en los siguientes rubros:

    - **TIC**: Utilizando Tecnologías de mejor privacidad (PET), Aplicando Privacidad desde Diseño (*Privacy by SDesign*) en las TIC*, software*, y aplicaciones, de programas de empresas públicas y privadas.
    - Comprendiendo el ecosistema del **Cómputo en la nube** y su impacto jurídico
    - **Sistema jurídico y normatividad**: Simplificado, preciso y de efectivo cumplimiento. Marco normativo de privacidad y de seguridad de la información. Destacando el tema de protección de datos como en el caso del Cómputo en la nube, de los datos del sector público y privado.
    - **Cultura digital**, que comprenda la importancia de la privacidad, la protección de datos personales y la seguridad de la información, sociabilizando y formando capital humano certificado para que en la toma de decisiones considere estos tres ejes fundamentales (privacidad, protección de datos y seguridad de la información), en los diferentes sectores.

Los **temas principales** de manera enunciativa y limitativa son los siguientes:

1. **TIC**:

Tecnología de mejor privacidad y privacidad por diseño

2. **Privacidad y Protección de datos personales**:

Como Derechos Humanos y Fundamentales, particularmente:

a) Cómputo en la nube,

b) Política de impacto a la privacidad aplicable a trabajos TIC de las empresas públicas y/o privadas.

3. Seguridad de la Información

4. **Prevención de delitos**.

5. **Derechos Humanos**:

A) Internet como acceso universal

B) Libertad de expresión

C) Libertad de prensa

D) Libertad de asociación

E) No discriminación y accesabilidad

F) Privacidad y Protección de Datos

6. **Datos personales**:

a) Contratación de cómputo en la nube de sector privado y público),

b) Datos Biométricos; en materia laboral, migratoria, criminal, etc.

c) Datos Clínicos; expediente electrónico, bases de datos clínicos, sector salud privado y público

d) Datos Financieros; Tarjetas de crédito, banca en línea y pago móvil.

e) Datos de identificación; poblacionales, electorales, DIN, cédula nacional de identidad, etc.

f) Comerciales y de *marketing*; firma electrónica y certificado electrónico

g) Datos de localización y seguimiento: GPS, RFID, dispositivos móviles, IP, cookies, etc.),

h) Responsables de protección de datos (sujetos obligados por ley, su capacitación),

i) Big data y minería de datos.

j) Redes sociales.

k) Certificado de Confianza Digital. Para tema de Privacidad y protección de datos, certificación de trabajos, sitios web y responsables de tratamiento.

7. **Prevención de conductas delictivas y delitos sobre la información o tecnologías**:
   A) Ciberterrorismo
   B) Ciberataques a sector publico
   C) Delitos de orden patrimonial; fraudes electrónicos, lavado de dinero *on line*, clonación de tarjetas, *phishing*, etc
   D) Delitos contra la Dignidad o integridad psicológica o emocional
      a) Prevención de *ciberbullying*, *sexting*, pornografía infantil.
      b) Suplantación de identidad
      c) Otros

8. **Propiedad Intelectual Digital:**
   A) Derecho al olvido
   B) Responsabilidad de los ISP

a) Conectividad, almacenamiento y gestión de contenidos

b) Relación estrecha entre Privacidad, Protección de Datos y Propiedad intelectual.

c) Estudio de Leyes internacionales referentes a la Propiedad Intelectual

9. Cultura Digital:

Capacitación y sociabilización del conjunto de temas a los diversos sectores de la Población, cubriendo los aspectos 3 mencionados.

CONSIDERACIONES FINALES

Es indudable que con el desarrollo de trabajos integrales como este, se lograría un impacto favorable en los diversos sectores de la sociedad; en el desarrollo económico, social, cultural, político y jurídico, en el sano ejercicio del presupuestal en materia de TIC que lleven miras a cumplir la ley y derechos fundamentales, legitimidad ciudadana, y respeto a los derechos humanos, entre otros.

En suma, recuperar de a poco la confianza entre las personas y de las personas al Estado y las empresas, sobre la base del respeto a la ley, es sin duda una clave para la mejora constante que buscamos para nuestra sociedad.

Beneficios que llegan por tres partes; cultura, legalidad y tecnologías, esto se traduce en cambio de actitud y desarrollo de la economía, del gobierno

digital y contribuye al potencial que de por sí tienen las TIC bien empleadas en los diversos sectores.

Con lo anterior, las nuevas tecnologías se convertirían en un mayor referente para gobierno y sector privado y sociedad en aportar soluciones integrales que lleven el enfoque multidimensional a nivel técnico, cultural y jurídico en temas de gran innovación y sobretodo privilegiando un enfoque social.

Sociedad tecnológicamente avanzada, Sociocibernética e Infoética: apuntes para un Modelo Legal.

Technologically advanced society, Sociocybernetics and Infoethics: notes for a Legal Model.

Yarina Amoroso
Vicepresidente FIADI

"…la Ciencia jurídica, ciencia madre como la filosofía, engendro y resultado natural de esta última, tanto más real cuanto más se aleja de las interpretaciones y las adiciones formales con que la desfigura muchas veces el desmedido afán de ciencia humano."

José Martí[1].

Resumen:

El estudio que se presenta se aproxima a la discusión de algunos conceptos básicos de la Sociocibernética y la Infoética considerando que son relevantes para los procesos de acción social y desarrollo humano en el contexto de la

[1] Martí, José: Revista Universal, México. 18 de junio de 1875. T. 6 pág, 233.

sociedad tecnológicamente avanzada a la que se le ha dado en llamar Sociedad de la Información y Sociedad de la Información las que demandan un código legal adecuado e invitan a repensar el Derecho como ciencia social a partir de la doble relación que tiene con las Tecnologías de la Información y las Comunicaciones (TIC) que dan paso a las Tecnologías Emergentes (TE) así como las interacciones con otras ciencias y áreas de conocimientos.

The study presented approaches to the discussion of some basic concepts Sociocybernetics and Infoethics, considering that are relevant to the processes of social action and human development in the context of a technologically advanced society that has been termed Information Society and the Information Society the demand proper legal code and invites to rethink the law and social science from the double relationship with the Information Technology and Communications (ICT) that lead to the Emerging Technologies (ET) as well as interactions with other sciences and areas of expertise.

Palabras clave: Derecho, Cibernética, Ciberespacio, Socio-cibernética, Infoética.

Law, Cybernetics, Cyberspace, Sociocybernetics. Infoethics.

Introducción

Se afirma que la mayor parte de los esfuerzos realizados por algunos científicos sociales durante los siglos XIX y XX, fueron orientados a desarrollar sus respectivas disciplinas a imagen y semejanza de las ciencias físicas y de la naturaleza.

Superado la primera década del siglo XXI se comparte el criterio de que las funciones de las ciencias sociales, tanto como áreas de estudio o como herramientas de saber aplicado, necesitan de un marco conceptual sólido que les permita disponer de una perspectiva válida y eficiente para un sistema social global y complejo.

Los males sociales que aqueja a la humanidad algunos de los cuáles han quedado expresadas en los Objetivos del Milenio y otros que han sido recogidos como metas de las Infoética en la Cumbre de la Sociedad de la Información representan un serio desafío para las ciencias sociales porque demandan, urgentemente, una nueva perspectiva internacional del desarrollo y la justicia social.

Basado en el estudio de algunas teorías y la aplicación social de las mismas a partir de modelos cibernéticos se afirma que la Sociocibernética, puede aportar una vista más dinámica y completa tanto para las actividades profesionales como para las preocupaciones teóricas de las ciencias sociales toda vez que ofrece un promisorio avance en los estudios de organizaciones y sistemas complejos.

La inseguridad ciudadana, la suplantación de la identidad, la invasión a la privacidad y la intimidad, la discriminación, la ineficiencia en la gestión administrativa, la corrupción y la imposibilidad de manipulación eficaz de un volumen de información digital que crece de forma exponencial, son entre otros algunos de los muchos otros males sociales que hoy aquejan a la

humanidad tecnológicamente avanzada lo que demanda con urgencia una nueva perspectiva internacional del desarrollo y repensar sus postulados porque inciden en la organización y las conductas sociales que se extienden más allá de los tradicionales límites nacionales y regionales e imponen nuevos espacios de realización de las relaciones sociales y jurídicas todo lo cuál conforma un fenómeno de dimensiones culturales y evoca cambio de paradigmas.

Sus efectos repercuten por doquier porque dichos males se globalizan y se afianzan en donde existen las condiciones para su reproducción y mutan haciendo un continuo de males, también amplifican males ancestrales como es el caso de la brecha digital que es una expresión más de la brecha social a causa de desigualdades en materia de justicia social y el derecho al desarrollo.

La información que a diario recibimos pone al descubierto o al menos llama la atención en que la sociedad no encuentra respuestas eficientes desde las áreas funcionales de las ciencias sociales. Quiénes se dedican a la investigación afirman que se impacta tanto a postulados teóricos como en la interpretación de resultados empíricos.

Por ello, cada vez se acepta de manera más amplia que la “ciencia” debe generar conocimientos que puedan ser traducidos en nuevos conceptos y en aplicaciones prácticas eficientes. Relacionado con lo anterior, se afirma que las ciencias sociales no sólo constituyen una representación lógica del mundo

real, sino que proporcionan, además, un mapa orientador y las herramientas necesarias para actuar en nuestro mundo.

La sociedad tecnológicamente avanzada es más dinámica y sujeta a cambio en menor tiempo, por lo que resulta necesario orientar los esfuerzos a formular un nuevo paradigma de las ciencias sociales que atienda las actuales demandas de variabilidad y complejidad de los sistemas sociales así como identificar los desafíos del desarrollo social internacional como metas comunes a alcanzar en todas las regiones y que orienten la acción social global a afianzar las conquistas sociales de la humanidad propendiendo a su desarrollo armónico para preservar la dignidad humana en condiciones de sostenibilidad, por ello es tan importante identificar los valores universalmente compatibles. De ahí la necesidad de un enfoque sistémico e integrador que incluya la vista de la Infoética que se asume como un estado práctico-evolutivo de la Etica y los vínculos con el Derecho.

Lo dicho hasta aquí delinea el desafío que se considera puede ser abordado con éxito desde la Socio-cibernética, aproximarse al tema exige identificar orígenes y aprehender los conceptos claves, así como atar los elementos de relación y aplicación de las ciencias sociales sin desconocer el desarrollo científico general y que se encuentra embebidos en las Tecnologías de la Información y las Comunicaciones (TIC) que dan paso a las Tecnologías Emergentes (TE).

Asumir lo anterior exige desarrollar por parte de los científicos sociales una aptitud y métodos de investigación y análisis propios acorde al carácter sistémico de la sociedad y propender a abordar los problemas por grupos multidisciplinarios para abordar los problemas desde una mirada intra, inter y transdiciplinar. Supone además comprender la naturaleza, fines y esencia sistémica del Derecho y posesionarlo en perspectiva de interoperabilidad. Es necesario incidir del ejercicio práctico y establecer puntos de observación que catalicen los procesos de retroalimentación como sistema que es.

1. Socio-cibernética: precursores y conceptualización.

La sociocibernética está considerada como una disciplina aún en construcción y tan dinámica como la sociedad misma. A criterio de sus precursores la Socio-cibernética involucra la aplicación de conceptos, métodos e ideas de lo que se ha llamado nueva cibernética o 'cibernética de segundo orden' en el estudio de sistemas sociales y culturales. (Geyer y Zouwen 1992).

El origen etimológico de la Sociocibernética expresa la conjunción de dos conceptos básicos: la raíz "socio" que denota todo lo referente al mundo de lo social, y el segundo, el de "cibernética" en este particular se restablece tres momentos de contacto:

- ✓ la acepción propia del término griego "kybernetes" para hacer referencia a la ciencia o arte con capacidad de guiar, orientar, intervenir las sociedades. Para Geyer la atención debe estar dada en el hecho en

que tales sociedades no son necesariamente de orden jerárquico. (Geyer 1995).

- ✓ la acepción propia del término en la dimensión de Cibernética según el uso dado por Ampere.

- ✓ la acepción propia del término en la dimensión y propuesta sistémica de Nobert Wierner en su libro *"Cybernetics. Or control and Comunication in the animal and the machine".*[2]

Al respecto, se coincide con Scott (2006) quien observa que históricamente, las teorías de sistemas y la cibernética se desarrollaron en diferentes contextos.

Es menester señalar, que inicialmente, Norbert Wiener, en 1948, se refirió a la Cibernética como la ciencia de la comunicación y control en los animales y en las máquinas, más adelante reconoció que se trata de la comunicación entre los hombres y las máquinas y entre máquinas.

Al estudiar la obra de Wierner "Cybernetics. The Human Use of Human Beings" en la cuál se amplían y precisan algunos temas abordados por él en su primer Libro se aprecia cómo se rectifican posiciones y se amplían alcances lo que

[2] Wiener, Norbert : *Cybernetics. Or control and Comunication in the animal and the machine.* John Wily & Sons. Nueva York. Año: 1948. 1ra. Edición.

favorece poderlo tomar como punto de partida para entender el presente de la sociedad en que vivimos. En correspondencia con los objetivos de este artículo, conviene apuntar que la obra de Norbert Wierner reconoce la Teoría de Sistemas[i] como parte de la Cibernética tendencia que se mantiene prácticamente en toda la literatura científica posterior a Wiener.

También se destaca que en la segunda edición de su libro Wiener reconoce que no inventó la palabra Cibernética como dejó entrever en la primera edición, declara que desconocía que había sido empleada antes por Platón y Ampere, pero declara el nexo de Cibernética con "*kubernetes*"… "de la cual se ha derivado en occidente gobierno y su derivados". Del mismo modo expresa, que parte de un capítulo ese libro fue publicado en *Philosofhy of Science*, al estudiarlo llama la atención la dimensión social de la cuál se sirve para explicar sus postulados y en la forma cómo lo expone. Ello incita a afirmar que la versión popular de su libro fundacional lo convierte en un precursor directo de la Sociocibernética.

Se comparte el criterio que la formación y desarrollo de la Sociocibernética como disciplina sigue los principios básicos de la teoría de sistemas y de la cibernética de comienzos del siglo XX pero sin desconocer sus antecedentes originarios, además de la importante contribución e influencia ejercida por las teorías de Niklas Luhmann y de Walter Buckley quien se considera un pionero en aplicar la perspectiva de los conceptos de la teoría de sistemas a los sistemas sociales, sostiene que la naturaleza específica de los sistemas sociales

es lo que los hace ser unidades viables de análisis, y útiles para la construcción de teorías (Buckley 1967).

En fecha más reciente, se sugiere que la Sociocibernética (Mulej, 2006) tiene como propósito central el conocer y comprender las complejas relaciones humanas y sociales. Otros estudiosos, estiman que "la tradición establecida por la Teoría General de Sistemas, conocida también por el nombre de Sociocibernética, puede aportar una perspectiva más dinámica y más completa tanto para las actividades profesionales como para las preocupaciones teóricas de las ciencias sociales"[3], lo que equivale a afirmar que "las funciones de las ciencias sociales, tanto como áreas de estudio o como herramientas de saber aplicado, necesitan de un marco conceptual sólido que les permita disponer de una perspectiva válida y eficiente para un sistema social global y complejo".[4]

El desafío principal de este marco de referencia es utilizar las coordenadas de la teoría general de sistemas en el análisis de la conducta y organización social. Al hacerlo, hay que tener en cuenta que aparecen problemas y paradojas tales como la que hay en las relaciones de la observación-observador-observado, el control y la evolución de sistemas que se auto-controlan, o la planificación en sistemas sociales donde las variables que se consideran no se alcanzan a abarcar en forma completa, ni por mucho que se amplíe el conocimiento de ellas sirven para un mejor control. La idea que el paradigma del control del sistema se puede aplicar a la conducta y organización social definidas como

[3] Darío Menanteau-Horta y Chaime Marcuello-Servós: Una perspectiva sociológica para la acción social y el desarrollo: avances de la Sociocibernética. 2006.

[4] Obis Cit.

sistemas sociales, representa entonces un paso significativo para aceptar la noción de planificación y acción social, de crítica e intervención social en tareas, funciones y servicios necesarios para el desarrollo social[5].

Otro ejemplo de transferencia teórica con la cual la Sociocibernética aspira a incrementar el conocimiento sobre los sistemas sociales está ilustrado por el concepto de autopoiesis desarrollado por Maturana y Varela (1972, 2000, 2002), en el campo de la Biología e incorporado al terreno de las ciencias sociales por Niklas Luhmann (1986, 1998).

De acuerdo con Luhmann, el proceso de comunicación se erige como una unidad central de los sistemas sociales siendo la acción social subsidiaria de los procesos de comunicación, los cuales constituyen el núcleo autopoiético de todo sistema social. Esta observación tiene importantes repercusiones epistemológicas distinguiendo al observador de lo observado y, de modo más especial, pone en alerta a las teorías preocupadas de la causalidad tradicional de los riesgos originados por los problemas de la circularidad del sistema.

Respecto a lo anterior conviene señalar que el científico social es parte de aquello que observa. No es un gestor de conocimiento aséptico y externo al mundo como observador que se declara neutral. No puede serlo. La estrecha interdependencia entre el científico como observador y el objeto observado es lo que emerge en el proceso de auto-referencia que representa una de las claves sobre las cuales está desarrollando la Sociocibernética actual que

[5] De Zeeuw: Cambio Social y el Diseño de Investigación. 1996.

sostiene que los sistemas sociales entendidos a partir de las claves y conceptos mencionados remiten a una revisión del conocimiento social necesario para estudiar la sociedad.

Todo conocimiento sobre la sociedad se retorna al sistema social de forma que varía las propias estructuras del sistema e incluso su comportamiento. Esta retroalimentación del sistema configura al sistema y las observaciones o mediciones que se hacen del mismo.

Los modelos sociales con los que se justifican investigaciones o políticas de intervención social operan sobre la base de la construcción de predicciones respecto al sistema y en la validación de los resultados científicos. Las reacciones ante esta retroalimentación configuran las interpretaciones de los actores sociales dentro del sistema. Así, el conocimiento del sistema social, sus estructuras y comportamientos están relacionados de manera que al actuar sobre uno de ellos, se reorganiza el sistema en su conjunto. Son, por lo tanto, procesos de adaptación y aprendizaje que exceden tanto al actor social como al científico. Todo esto después se concreta en procesos e interacciones sociales con consecuencias directas en todas las áreas de lo social, lo económico y lo político, por ende en el Derecho.

Se reseña además, que el comienzo de la Sociocibernética fue objeto de críticas y algunas objeciones. La sociedad tecnológicamente avanzada actual que tuvo en parte su origen u hito evolutivo en la década de los años 1940, recibió una fuerte influencia de las ingenierías y ciencias aplicadas, lo cual propulsó la construcción del primer computador y otros avances tecnológicos.

Además de esto, los principios conceptuales de la "cibernética clásica" contribuyeron también a despertar el interés de la sociología y de otras ciencias sociales en el estudio de la teoría general de sistemas y prestar atención a la creciente complejidad del cambio y desarrollo de los sistemas sociales.

En fecha tan temprana como el año 1948 quedó establecida la relación de la Cibernética con el Derecho dando origen a un área de conocimiento y desarrollo que mostraba una doble relación de objeto y medio; nace así lo que se conoce como Informática Jurídica y más recientemente Derecho Informático. Sin embargo los nexos se mantienen entre luces y sombras que se expresa en una dimensión incompleta de las vistas de organización, dirección y control se la sociedad tecnológicamente avanzada y peor aún la discontinuidad en la construcción de la llamada Sociedad de la Información y su hito de Sociedad del Conocimiento sobre bases de posiciones tecnocráticas en lugar de un enfoque socio-técnico.

2. Sociocibernética y desarrollo social.

La relación entre las funciones del desarrollo social y la Sociocibernética está profundamente enraizada en la naturaleza de los procesos de cambio organizacional, mejoramiento de las condiciones de vida y la metodología cibernética.

La noción de desarrollo social y la cibernética surgen como nuevas perspectivas para la búsqueda de mejores formas y procedimientos para resolver problemas. Aunque el concepto de desarrollo tiene una historia (Rist 2002) y una densidad de contenidos polisémicos y polémicos, podemos afirmar, sin embargo, que cuando el desarrollo se define en términos de desarrollo social, implica la presencia de un diseño de intervención para mejorar las condiciones humanas. Esto es lo que permite diferenciar el concepto de desarrollo social como una herramienta para el bienestar individual y colectivo de otras formas de cambio evolutivo o de sólo crecimiento económica. Al decir de (Espejo 1996) “el aprendizaje está relacionado con el proceso de resolver problemas” que equivale a decir que con el empleo de la metodología cibernética se puede descubrir, comprender y aprender acerca del mundo y de sistemas sociales. Por ende la Sociocibernética, es una herramienta para asimilar realidades y esto debería ser, por cierto, un desafío común y algo compartido por la metodología de las ciencias sociales del siglo XXI.

La aplicación y relevancia de la Sociocibernética en el campo de la acción social radica en las relaciones existentes entre los procesos de comunicación, intercambio de información y organización social. Estas relaciones permiten a los sistemas recibir y utilizar información lo que ayuda a que los sistemas sociales puedan cambiar y ajustarse al medio y condiciones externas. La creciente complejidad de la sociedad contemporánea incrementa aceleradamente la demanda de información y ello contribuye a hacer del rol de los científicos sociales una función esencial para disponer de una

comunicación transparente, una organización social justa, una acción colectiva eficiente, y un cambio social adecuado.

Los procesos sociales y los problemas que afectan los sistemas sociales se caracterizan por no ser estáticos. Al contrario, ellos pueden ser sujetos de cambio y mejoramiento cuando se incrementa el conocimiento, se cambian las conductas y se toman las medidas apropiadas. Un mayor conocimiento de la sociedad y una mejor comprensión de las organizaciones en sistemas sociales complejos son fundamentalmente necesarios para la formulación de políticas públicas y la estructuración de programas nacionales e internacionales de desarrollo social.

La naturaleza recursiva de los sistemas sociales permite y aun requiere que se reconozca la importancia de cada individuo en cuanto es una persona humana dentro de un sistema.

Esta condición de sistema lleva consigo la aceptación de valores ético-sociales que usualmente se observan conectados a un tipo de cambio social con propósito, o desarrollo. Según Maturana y Varela (1988), la dimensión axiológica de los seres humanos es clara al considerar que “En el hombre como un ser social, todas sus acciones, aún aquellas individuales como expresiones de preferencias o rechazos, afectan constitutivamente las vidas de otros seres humanos, y por eso, tienen un significado ético.”

Se considera como un precursor práctico de la Sociocibernética a Stanford Beer quién en toda su obra proporciona una clara aplicación de la Cibernética

al análisis de sistemas sociales y desarrollo de soluciones para problemas de desarrollo nacional y otras unidades mediante lo que él definió como Modelo de Sistemas Viables, Beer (1975). De alta relevancia para la disciplina es la noción de Beer de considerar el cambio social planificado, como una herramienta para mejorar las condiciones de vida de todos los miembros de un sistema social (1975; 1972).

Un intento de aplicación del Modelo de Sistema Viable tuvo lugar en Chile a comienzos de los años 1970 con el propósito de elaborar, en un tiempo real, información y herramientas que facilitaran la toma de decisiones para la economía e industrias del país. Éste, llamado también "Proyecto Cibersin[ii]", por la combinación de las palabras "cibernética" y "sinergia", ha sido considerado el primer esfuerzo para implementar un programa de Sociocibernética en América Latina y un referente válido para desarrollar aplicaciones de Gobierno Electrónico y de Gobierno de la Información en base a una visión sociotécnica de la informatización de procesos de administración y gobierno con apego a postulados infoéticos.

Tal afirmación se basa en considerar los objetivos básicos y generales del modelo de Sistema Viable se pueden resumir en los siguientes principios operacionales:

(1) Incorporar la ciencia y la tecnología a los procesos de comunicación y mecanismos de decisión para facilitar la planificación, la organización, y el desarrollo;

(2) Promover la comunicación continúa y transparente entre un gobierno elegido y todos los miembros del sistema social;

(3) Aplicar una metodología que permita la comunicación entre todos los sectores del sistema para hacer posible la organización y el aprendizaje sociales tendientes a resolver los problemas y desafíos del desarrollo social;

(4) Facilitar y estimular la participación social que refleje plenamente las necesidades y la voluntad de las personas, desde la participación ciudadana, la cual es la piedra angular de la legitimidad de un gobierno o de cualquier otra forma de poder político.

(5) Promover el desarrollo social por ser éste un mecanismo funcional esencial para el mejoramiento del bienestar humano.

Los conceptos motores del proyecto para atender la complejidad del sistema chileno fueron fundamentalmente tres: el de viabilidad, el de recursión y el de autonomía. Estos principios fueron incorporados dentro de un modelo neurocibernético basado en la idea que el manejo de una organización o sistema es una función de control, orientación y guía.

Esto es particularmente importante cuando se trata de programas de desarrollo social donde las prácticas de participación de las bases son esenciales para el logro de las metas y objetivos de dichos programas. En la literatura relacionada con programas de desarrollo internacional y en experiencias nacionales y locales sobre desarrollo de comunidades, el capítulo sobre participación de los miembros de esos sistemas es bien conocido y recomendado por todos los científicos sociales.

Aunque la experiencia de este proyecto en Chile fue breve y terminó abruptamente con el golpe militar de 1973, se reconoce que los objetivos y

componentes principales de esta iniciativa tienen un merecido valor conceptual y ofrecen un importante aporte intelectual y práctico para quienes tienen interés en el estudio de los problemas sociales y las posibles herramientas para extirparlos.

En décadas recientes el Modelo de Sistemas Viables ha capturado el interés académico de la Sociología, Ciencias Políticas, Relaciones Internacionales y también su uso práctico por profesionales de otras disciplinas para atender problemas usualmente encontrados en la administración de empresas, en la organización industrial y en los cambios necesarios para el desarrollo de las naciones. Espejo y Harnden (1989) describen la aplicación de este modelo a problemas específicos en las áreas del cambio social y desarrollo. Beer (1989), por su parte, informa la utilización del Modelo de Sistemas Viables en el campo internacional incluyendo Inglaterra, Canadá, Europa, Estados Unidos, Australia, Nueva Zelanda, Chile y América Latina. Poco o nada se ha empleado en el área del Derecho, aquí se hace la invitación a buscar el por qué que es parte de la continuidad de este estudio.

3. Socio-cibernética y desafíos del desarrollo social internacional. Apuntes para un Modelo de Marco legal.

En sede de la sociedad tecnológicamente avanzada que hoy se conoce indistintamente como "Sociedad de la Información" o "Sociedad del Conocimiento" e incluso algunos la identifican como la "Era digital", o simplemente Ciberespacio la Sociocibernética puede ser una vía para buscar

soluciones para enfrentar y ordenar procesos destinados a solventar algunos de los males que se ha generado por la incidencia social de las TIC y las TE.

El primer paso para comprender el fenómeno es reconocer una convergencia de dos escenarios: el “mundo real” extendido en el “mundo virtual”, en este último el hombre interactúa con información digital y los valores espacio, tiempo y cosas a los que estamos acostumbrados cambian.

Al decir del Dr. Vittorio Frosini "(...) Esta es la nueva forma de la información, asimila en nuestro tiempo de civilización tecnológica, después de las formas anteriores de información verbal o gestual, simbólica con dibujos y con escritura, y más tarde con la imprenta y con los medios de transmisión eléctrica, hasta llegar al actual tratamiento (...)[6]", en este caso la información digital en virtud de la cuál la humanidad ha ido identificando un cambio en los paradigmas en cuanto al soporte informacional pero es de significar que al aproximarnos al fenómeno nos encontramos que una de las características es la convergencia en los medios de transmisión de información y soportes a través de los cuáles se almacena, procesa y trasmiten diferentes tipos de información (texto, imagen y sonido) a partir de las cuáles se genera el mensaje.

Por lo tanto, se ha definido al mensaje hoy en día "como una información trasmitida en la cuarta dimensión, aquella de la cognocibilidad pura, similar a la de la memoria y el pensamiento humano, ya que la elaboración de los datos por obra del computador se produce a una velocidad que se mide en

[6] Vittorio Frosini: Cibernética, Derecho y Sociedad. Tecnos, Madrid, 1978.

millonésimas de segundos, y su transmisión en tiempo real anula las distancias, el espacio y el tiempo (...)[7]".

Así el desarrollo de la infraestructura mundial de información ha transformado nuestro entorno común, especialmente en lo que se refiere a la generación y transmisión de datos, información y conocimiento, convirtiéndose a su vez en generador de nuevas fuentes y formas de realización de empleo, por ende trasciende a nuestra vida cotidiana.

Cada día la información se consolida como bien social, económico y jurídico autónomo. En cuanto a su forma, se ha separado de su continente tradicional: el paradigma papel, que hoy convive con el soporte digital; sin embargo la información se ha independizado de los mismos sin perder su identidad y su función.

Por otra parte, a la información se le reconoce valor como materia prima fundamental en el cuarto sector industrial. Se identifica además, como un recurso estratégico para el desarrollo; de manera tal, que los cambios estructurales son palpables en términos de indicadores de crecimiento económico, por ello la distinción entre países inforricos e infopobres que es una de las vistas de la brecha digital y del derecho al desarrollo.

También se reconoce, que la aplicación de las nuevas tecnologías de la información y la comunicación al entorno social en general es fuente de un sector productivo en tanto genera bienes y servicios y modos diferentes de realización del comercio internacional.

---

[7] Amoroso, Yarina y otros: Diccionario de Jurismática, La Habana, 2000.

A nivel social, surgen oportunidades sin precedentes para la comunicación lo cual favorece extraordinariamente procesos de generación e intercambio de información. Pero, si el ciberespacio es un espacio de todos, como se ha dado en decir, se debe hacer de él también un espacio de la democracia multicultural y del multilingüismo.

Por otra parte, también se señala que el empleo razonable de grandes sistemas de información en interés de la sociedad, así como la protección segura de toda la información son factores pre determinante de una actitud de respecto ante las posibilidades que brindan las tecnologías de la información y la comunicación, y éste debe también considerarse como axioma ético.

Entre los componentes que integran esta estructura global de la información identificamos al factor humano; a la información que como se dijo es el elemento estratégico y la infraestructura material de conexión e interoperabilidad además del software, como elementos que constituyen los elementos indispensables a través de los cuales se materializa esta realidad.

Todo ello deriva en consideraciones ético-jurídicas sobre el tratamiento digitalizado, el uso y la conservación de la información. Dos posiciones prevalecen en cuanto a la potencialidad del Derecho como instrumento regulador de las situaciones a que da lugar la incidencia social de las tecnologías de la información y las comunicaciones, y especialmente el fenómeno de las redes de alcance global.

La primera de ellas, encabezada por la conocida frase de "nada nuevo hay bajo el sol", asevera la eficacia de los instrumentos jurídicos clásicos (existentes aún desde antes de la aparición de Internet) para dar solución. Esta es la variante de articulación de formas clásicas junto al diseño de lo que generalmente llamamos tecnología, es una mistura reactiva desde el punto de vista de articulación del orden legal.

Dentro de esta primera corriente, se ha presentado como piedra angular de todo el ordenamiento jurídico, a los Principios Generales de Derecho, los que, constituyendo las reglas fundamentales de asiento al sistema, proveen una serie de soluciones expresas del Derecho positivo a la vez que pueden resolverse, mediante su aplicación, casos no previstos, que dichas normas regulan implícitamente.

La segunda posición, sostiene, atendiendo al carácter novedoso de las situaciones a que dan lugar las realidades tecnológicas, la marcada dificultad e inoperancia, de los instrumentos jurídicos tradicionales para resolver situaciones propias del ámbito natural del fenómeno en el Ciberespacio.

Pero en todo caso no se niega que el Derecho deberá ser el instrumento orientado, como objetivo fundamental, a preservar la dignidad humana en la era digital y que como medio institucional de regulación de las relaciones humanas, no es ajeno, es más, no puede ser ajeno al fenómeno.

La pregunta entonces es ¿qué Derecho? El problema de profunda raíz política requiere además de una meditada reflexión académica y de acciones prácticas.

Y para ello, varios y diversos operadores deberán actuar como diversos son los escenarios en los que hay que desarrollar tales acciones para la toma de decisiones a favor de interés social y el bien común. Otro aspecto a tener en cuenta es la necesidad de generar instrumentos internacionales especialmente desde las organizaciones internacionales de carácter público como es el caso del sistema de órganos de Naciones Unidas.

Para contribuir al debate se abordan algunas interrogantes que ayudan a evidenciar aristas del problema:

¿Los instrumentos jurídicos existentes (leyes, principios contractuales, procedimientos administrativos y jurisprudencia) son suficientes para propiciar el desarrollo armónico de los procesos tecnológicos y eficientes en cuanto a los avances en la tecnología de la información en general se refiere, y su producción y uso en particular?

En el contexto de los valores e intereses jurídicos generales en una sociedad funcionalmente adecuada, no puede ser excluido el hecho de que los instrumentos existentes necesiten algunas modificaciones o ajustes. Puesto que el marco jurídico es anterior, es probable que la ley existente no pueda ser aplicada en todo o es al menos confusa con respecto a varios aspectos de producción y uso de tecnología de la información, pero no todo el Derecho es ineficaz.

Por ejemplo las condiciones económicas de la producción tecnológica parecen estar favorablemente influenciadas por instrumentos jurídicos existentes, tales es el caso de las decisiones judiciales sobre el Derecho de Competencia.

Pero en otros campos, además del económico, la efectividad de instrumentos jurídicos muestra ciertas deficiencias, tal es el caso de la legislación civil sobre la estandarización de la calidad de los productos de la tecnologías de la información y la correspondiente responsabilidad o los instrumentos de Derecho Administrativo y Penal en cuanto a la vulnerabilidad y salvaguarda de la información se refiere, más resulta importante resaltar que los valores protegidos siguen estando protegidos y el Derecho es capaz de dar una respuesta ante un quebrantamiento de la legalidad.

También es cierto que algunos conceptos jurídicos tradicionales comienzan a resultar estrechos y que surgen interrogantes tales como: ¿la información es una mercancía o un bien? E incluso más: ¿tiene una función social?

Tratar la información exclusivamente como mercancía es un error. La información debe ser tratada en diversas dimensiones tales como: un derecho, un documento y también como bien. La misma desempeña un papel muy importante en la educación, en la ciencia, en las relaciones sociales, en la representación, en la preparación e implementación de fundamentos y decisiones, y dado su importancia social e incidencia para el desarrollo, su significado económico, la misma reclama un status legal *sui géneris*.

La legislación de intereses relacionados con el tema no puede ser única por los valores polivalentes que tiene la información con relación al sujeto que la genera y al receptor que la recibe, manipula, procesa o conserva, por eso se

formula en una legislación especial para los temas de intimidad, propiedad intelectual y las reglas para el intercambio electrónico de datos.

Finalmente me quiero referir a la relación Redes y Derechos, dado que la misma una independencia particular en el contexto del Derecho de la Informática y la propia Infoética, ya que en las redes se reproducen todos los problemas primarios objeto de estudio del Derecho de la Informática, tal como los relacionó Michel Vivant en su conferencia ¿Qué es el Derecho para las redes sin fonteras?[8]:

"- redes y libertades;
- redes y propiedad;
- redes y responsabilidad;
- redes y fraude;
- y, más especial, redes y contratos."

Por otra parte, la transformación de las dimensiones de tiempo y espacio en el ciberespacio está generando una tendencia a declarar la "inoperabilidad" del Derecho ante estos problemas, lo cual constituye una incitación al caos y nada en la sociedad puede existir en estado de anomia y el Ciberespacio es una dimensión de realización de las relaciones sociales y por ende de hecho jurídicos.

Se coincide con Vivant en que (...) "Sobre las redes, una falsificación se mantiene una falsificación y una palabra de incitación al rencor racial se mantiene una palabra de incitación al rencor racial".

[8] Vivant, Michel: Que es el Derecho para las redes sin fronteras? Conferencia Magistral. V Congreso Iberoamericano de Derecho e Informática, La Habana, 1996.

Más exactamente, es cierto que el Ciberespacio es un espacio de libertades pero también de responsabilidades, entre ellas las jurídicas; y en el que los derechos tienen el límite que le impongan otros derechos, y en el que los valores e interés social tienen prioridad sobre los valores e intereses individuales.

Otros estudiosos como Jean Pierre Chaumoux, han abordado también el tema de los aspectos jurídicos de la información, todo lo cual ha dado origen a nuevas instituciones jurídicas o al planteamiento de reconsiderar algunas instituciones tradicionales del Derecho como el documento y los elementos constitutivos de su validez y valor probatorio, a partir de los nuevos soportes informacionales sobre los cuales se realiza la transmisión y la difusión de la información[9].

Pero esta realidad no debe ser analizada ajena a las diferentes circunstancias en las cuales surgen y se realizan estos instituciones jurídicas, dado el desigual desarrollo tecnológico del concierto de naciones, la ausencia de regímenes jurídicos internacionales y nacionales aplicables a las nuevas relaciones socio-jurídicas, así como un desarrollo doctrinal dispar, todo lo cual trae aparejado relaciones de dependencia tecnológica y doctrinal, un proceso paulatino de transculturación y el cuestionamiento de en cuanto a la validez del concepto de soberanía y la propia existencia de los estados-nación al identificarse un

[9] Chaumoux, Jean Pierre: Consideraciones sobre la información. París. 1980.

nuevo espacio sin fronteras y en el cual algunos vaticinan la inoperancia del Derecho.

Tales presupuestos si bien conducen acertadamente a una reevaluación y modernización del Derecho para su re-diseño, no dejan de ser una brecha también para imponer reglas de Derecho; en otras palabras la preconizada des-regulación como consecuencia de la incidencia social de las tecnologías de la información y la comunicación no es más que una forma de regular ajena al proceso actual de elaboración del Derecho y desconociendo realidades sociales y políticas diferentes, evitando incluso que se concurra para la toma de decisiones propias.

El tema de los nombres de dominio aunque ha evolucionado, podría ser un buen ejemplo de lo que se ha planteado. No es éste un tema exclusivo del ámbito de la propiedad intelectual como se quiere ver en su relación comercial, es y mucho más importante un tema también de soberanía sobre el cual hay mucho que reflexionar y proponer soluciones.

Es de destacar en sentido general, que consustancialmente a este fenómeno desde el Derecho: prácticas judiciales, normas jurídicas y doctrina, se está generando todo un proceso de cambio en importantes instituciones jurídicas tradicionales y asistimos al surgimiento de otras nuevas devenidas de las emergentes relaciones socio-jurídicas generadas de la incidencia social de las nuevas tecnologías de la información y la comunicación, pero es importante propiciar la armonización en los procesos de elaboración legislativa y la solución de conflictos, estamos asistiendo a la consolidación de nuevos usos y

costumbres, y porque no decirlo a un nuevo “Derecho de Gentes”, pero construyámoslos entre todos.

La sociedad tecnológicamente avanzada que hoy se manifiesta en el Ciberespacio no convive ni conviene hacerlo en un espacio de "no derecho" por ello urge emprender acciones más coordinadas en el seno del Sistema de Naciones Unidas para la búsqueda de soluciones más efectivas y eficaces para el concierto de naciones cuál expresión de soberanía.

Conclusiones:

Acogerse a los principios de Infoética y practicarlos, contribuirá a fomentar las Relaciones de Confianza y Gestión de la Seguridad en la era digital

La Sociocibernética expande la perspectiva de intervención y control de sistemas por la vía de la planificación social introduciendo la presencia y participación de múltiples actores en el sistema social.

Asumir la Sociocibernética ayuda a superar una visión Tecnocéntrica de los procesos de informatización y asumir una visión Sociotécnica de los procesos de informatización.

Los enfoques sociocibernéticos en los proyectos de informatización facilitar el diseño de los mismos en términos de conexión e interoperabilidad en

correspondencia con las buenas prácticas en la gestión de datos enlazados para favorecer la necesaria transparencia en los procesos de la Administración.

Una lectura actualizada de la Informática Jurídica nos obliga a ocuparnos de delinear y diseñar el código que se corresponda con el Principio de procedencia y orden natural para la Continuidad Digital, y su correspondencia con el Principio de Equivalencia funcional.

"CIUDADANÍA DIGITAL: Hacia una nueva forma de ejercicio de la ciudadanía en la Sociedad Red"

Guerrero Carrera, Jacqueline[10]
Universidad de Las Américas
Calle Granados y Colimes, esquina, Quito, Ecuador
Email: jguerrero@udla.edu.ec

Resumen:

Conforme lo ha expresado Manuel Castell, visionario de la Sociedad Red, Internet ha potenciado la participación ciudadana, permitiendo un acercamiento entre el gobierno y los ciudadanos, y logrando una participación interactiva permanente, especialmente en las redes sociales y en la comunidad virtual en general. Así, en el marco de la Sociedad de la Información o Sociedad Red se vislumbra el surgimiento de una nueva forma de ciudadanía, especialmente en función de las conductas políticas de los internautas.

Es preciso también analizar si las competencias ciudadanas son las mismas de la sociedad analógica o si estamos frente al surgimiento de un nuevo ciudadano digital, dotado de derechos y obligaciones, pero sobre todo con competencias particulares para la comprensión de los temas relativos a las TIC y las conductas asociadas a las mismas.

---

[10] Docente tiempo completo, Directora de la Facultad de Derecho de la Universidad de las Américas, Quito – Ecuador

Una aproximación al concepto de ciudadanía digital y el establecimiento de los alcances de la figura emergente del ciudadano digital, constituirán los ejes principales de la ponencia.

Palabras clave: ciudadanía digital, sociedad red, democracia electrónica.

I. Introducción

En la encuesta de Gobierno Electrónico de Naciones Unidas "E-gobierno para el futuro que queremos", difundida en el 2014, el Ecuador se ubicó en el grupo de los 20 países de América con un rango de desarrollo medio alto en materia de gobierno electrónico. Al tiempo, en mayo de 2014 se presentaba el Plan Nacional de Gobierno Electrónico 2014-2017[11], cuya elaboración estuvo a cargo de la Secretaría de la Administración Pública, y en el cual se define un modelo de gobierno electrónico para el país, así como la estrategia para su implementación.

El Plan responde a la realidad actual de una sociedad cada vez más interconectada y globalizada, y determina que los actores fundamentales del Gobierno Electrónico son los ciudadanos y ciudadanas, pues aquél es un medio de participación e interacción que permite el adecuado ejercicio de sus derechos y obligaciones[12]. Se considera que el Gobierno Electrónico permitirá acercar al país a la democracia 2.0, para lo cual la participación democrática de los ciudadanos en un entorno virtual es fundamental.[13]

[11] http://www.gobiernoelectronico.gob.ec/PlanGobiernoElectronicoV1.pdf
[12] Plan Nacional de Gobierno Electrónico 2014-2017, Pág. 13
[13] Idem, Pág. 17

En este contexto, merece especial atención la investigación acerca de los miembros de la sociedad digital o los denominados ciudadanos digitales, por lo que el presente trabajo, haciendo un ejercicio de introducción al concepto de la ciudadanía digital, abordará temas relativos a las competencias ciudadanas en el entorno virtual, la inclusión digital, las comunidades virtuales, entre otros. Finalmente, la conclusión evidencia que la ciudadanía digital es un concepto emergente que enfrenta múltiples desafíos, por las complejidades inherentes a los elementos que la conforman.

Ciudadanía digital: un concepto unívoco

Resulta difícil abordar el concepto de ciudadanía desde un solo postulado, pero para los fines del presente trabajo interesa establecer que la ciudadanía deriva de la pertenencia de un individuo a una comunidad y se traduce en el comportamiento de éste en el marco de la sociedad a la que pertenece, bajo el cumplimiento de ciertos requisitos. Así también, el concepto siempre ha estado estrechamente vinculado con la participación ciudadana, con el empoderamiento por parte de los ciudadanos de las prácticas políticas, en un marco de garantía del Estado del respeto de los derechos que permite tal participación. Finalmente, la ciudadanía se ha circunscrito a los límites del Estado, en definitiva a un espacio territorial.

Esta clásica forma de entender a esta institución trascedente, se redefine si se formula una simple pregunta: *¿qué representa hoy ser un ciudadano*? La respuesta necesariamente debe contextualizarse en el ámbito de la Sociedad de la Información y en el nuevo paradigma de ésta: la Sociedad Red.

Emerge entonces la *ciudadanía digital* como una institución que se construye con la definición de distintos roles como: el ejercicio de los derechos ciudadanos propiamente, el activismo y la participación; que precisa de unas competencias para su ejercicio y un espacio para su desarrollo, siendo éste último el aspecto que se analiza a continuación.

Comunidad Virtual

Cuando Mcluhan acuñó su famosa idea sobre la *aldea global* si bien pudo anticipar el potencial de la interconectividad de los seres humanos a nivel mundial, no podía dimensionar aún las profundas transformaciones que tal interconectividad produciría en instituciones tan clásicas como la ciudadanía. Hablar de una aldea global es hacer referencia a una comunidad mundial virtual, a la que podemos pertenecer todos, no sólo porque estamos interconectados sino por las prácticas comunes, como el activismo social.

Si bien para algunos autores "las llamadas comunidades virtuales no pueden considerarse comunidades sino seudocomunidades o metáforas de las comunidades reales, debido a la debilidad y precariedad de las relaciones sociales que las definen"[14], es indudable que desde el aparecimiento del Internet y con el vertiginoso desarrollo de sus aplicaciones, que han redefinido de forma inimaginable las formas de relacionarse de los individuos, se empezó a vislumbrar el surgimiento de un nuevo espacio opuesto al analógico, que se ha desarrollado en un mundo *virtual*.

[14] Harasim, McLaughlin, Osborne y Smith, citados por Robles, José Manuel en *Ciudadanía Digital,* UOC, Barcelona, Pág. 27

Estos nuevos espacios de interacción social se han visto representados con claridad en las denominadas *redes sociales,* que aglutinan a cientos de internautas con intereses y prácticas comunes, sin importar su pertenencia a una comunidad analógica en particular, pues en el espacio virtual no importa la nacionalidad sino el interés común, así en un momento determinado pueden haber miles de internautas defendiendo los derechos de la naturaleza o de un grupo vulnerable.

Algunas de estas redes tienen un particular empleo en asuntos políticos, como twitter, generando efectos directos en las prácticas políticas, sin embargo un aspecto relevante es la legalidad del empleo de estos medios en determinadas actividades de la vida democrática.

El espacio digital ha sido cuna entonces para el surgimiento de una *comunidad virtual*, que lejos de ser un espacio etéreo ha potenciado la participación e interacción de sus miembros, con la única limitación de la percepción que éstos tengan sobre el uso de las herramientas y aplicaciones disponibles y la real capacidad que tengan para hacerlo.

Un tipo de ciudadanía universal

La ciudadanía universal es un concepto que no necesariamente ha estado asociado al tema tecnológico, sino más bien ha derivado de la necesidad de movilidad humana y la eliminación de los límites estatales para el reconocimiento y garantía de los derechos individuales. Sin embargo, a propósito de la característica de aterritorialidad de Internet y su naturaleza global, la ciudadanía digital se convierte en un ejemplo y muestra real de

aquella, pues permite que ciudadanos de diferentes países del mundo confluyan en un espacio virtual para realizar actos de carácter político.

Ciudadanía digital, ciberciudadanía o e-ciudadanía son términos que se han utilizado en los últimos tiempos, con diferentes acepciones y alcances. Ciertamente, la definición de la ciudadanía digital no ha sido única y en el espectro que contiene las variadas propuestas se incluyen aquellas de connotación política y hasta las que tienen relación con la educación.

La concepción educativa de la ciudadanía digital define a ésta como el conjunto de normas de comportamiento relativas al uso de la tecnología[15], siendo entonces necesario pensar en la educación como una estrategia para preparar a las personas, especialmente a niños y jóvenes, para insertarse en la sociedad digital. Así por ejemplo, a partir de los estándares NETS[16] se pretende formar estudiantes tecnológicamente competentes, que puedan vivir en un mundo interconectado o en la denominada Sociedad Red.

Por otro lado, partiendo del hecho evidente de que el uso de la tecnología ha cambiado la forma de relacionamiento en la sociedad y ha redefinido la relación entre el gobierno y la ciudadanía, y que Internet, de forma particular, ha permitido el surgimiento de un nuevo espacio para el

---

[15] Traducción realizada por EDUTEKA del Artículo original “Digital Citizenship, addressing aprópiate technology behavior" escrito por Mike S. Ribble, Gerald D. Bailey, y Tweed W. Ross (http://coe.ksu.edu/digitalcitizenship/). Publicado en los números 1 y 2 del Volumen 32 de la revista Learning & Leading with Technology (http://www.iste.org/LL/32/1/index.cfm). Disponible en: http://www.eduteka.org/CiudadaniaDigital.php

[16] Estándares Nacionales de EEUU de Tecnologías de Información y Comunicación.

debate político, el activismo social, la defensa de los derechos, entre otros, se deriva el desarrollo de un nuevo concepto de ciudadanía, que involucra a todos los ciudadanos del mundo que tienen una participación en Internet, pero hace alusión específicamente al comportamiento político de los internautas[17].

Siguiendo el pensamiento de Robles[18], en cualquiera de los casos está claro que la ciudadanía digital es el resultado de un proceso de construcción social, en el que se requieren dos elementos: *objetivos y subjetivos,* los cuales determinan el grado de evolución de la institución en una determinada sociedad.

Los elementos objetivos que permiten hablar de ciudadanía digital están asociados a los medios que crean el entorno en el que aquella se puede desarrollar, y entre otros son:

- *Infraestructura:* Internet y el acceso a éste medio, siendo importante entonces el nivel de penetración del servicio en la población.
- *Herramientas, aplicaciones y servicios:* son aquellos recursos que ofrece Internet para desarrollar actividades de activismo social o políticas, siendo importante temas como la regulación de la propiedad intelectual y los riesgos de control político.

[17] Robles, José Manuel, Ob. Cit.
[18] Idem, Pág. 31

Por otro lado, los elementos subjetivos están relacionados con la actitud, la habilidad y en definitiva la actuación de los usuarios, siendo algunos de ellos los siguientes:

- *Percepción de uso:* la potencialidad de uso que identifica cada persona en los recursos de Internet, especialmente con fines políticos.
- *Alfabetización digital: o* competencia en el manejo de información (CMI) que implica actitudes, habilidades y destrezas para el uso de la información que se ubica en Internet, incluyendo los recursos.

II. Competencias para la ciudadanía digital

La democracia se asienta en la premisa de que los ciudadanos, titulares de derechos, tengan conocimientos, habilidades y actitudes, es decir competencias, para ejercer sus derechos y poner en funcionamiento las garantías que se han fijado para la defensa de los mismos. Se habla entonces de competencias ciudadanas para vivir en una sociedad democrática.

Tratándose de la ciudadanía tradicional, el tema de los requisitos para ostentarla está superado, pues el ejercicio ciudadano no es automático, sino que precisa de una activación conforme lo prevé la carta fundamental de cada Estado. Sin embargo, más allá del cumplimiento de ciertos requisitos, cada día se discute con más fuerza el tema de las competencias para ser ciudadano, pues sin duda ser ciudadano es una tarea compleja, que no se limita al ejercicio del derecho al sufragio.

En este contexto, una de las principales competencias para ser ciudadano está vinculada con la formación de los mismos; el nivel de educación queda superado si se considerara que en la actualidad para lograr una participación activa de los ciudadanos, especialmente en temas inherentes a la vida democrática, se requiere que los ciudadanos estén bien informados, que ubiquen, procesen y comuniquen información, es decir que puedan solucionar problemas de información.19 Para lograr este fin el uso de las TIC es indispensable, es decir no se puede alcanzar el cometido anterior sin un medio eficaz y las herramientas tecnológicas resultan ser altamente poderosas para permitir el acceso a la información, la generación de espacios de discusión y expresión de ideas y la promoción de la participación activa.

En relación con la ciudadanía digital las competencias ciudadanas son las mismas pero con algunas variantes, así la principal competencia que exige la ciudadanía digital tiene relación con el manejo de información y para ello es indispensable hacer referencia al alfabetismo informacional e incluso al denominado "Nuevo Alfabetismo", que "incluye la competencia en manejo de información (CMI), manejo de interactividad, hipertexto, multimedios, imágenes e íconos, tablas y gráficas, datos estadísticos; y alfabetismo en medios".[20]

---

[19] Para solucionar un problema de información se requiere realizar algunas actividades como: poder ubicar el área al que pertenece el tema de investigación, disponer de los descriptores adecuados o palabras que permitan realizar las búsquedas, definir cómo se realizará la búsqueda y las fuentes a las que se apelará, previa valoración de las mismas. Finalmente, debe existir la capacidad de procesar la información recolectada, emplearla para el fin que motivó la búsqueda y de ser el caso comunicarla.

[20] Eduteka, La competencia en manejo de información (CMI) y las competencias ciudadanas, disponible en http://www.eduteka.org/CMICiudadania.php

Este aspecto es de especial trascendencia pues permite explicar uno de los temas de mayor preocupación en relación con la Sociedad de la Información, en la que al parecer se reproducen las desigualdades de la sociedad analógica, especialmente las derivadas del nivel de educación de los individuos y las acciones asociadas a esto como la participación.[21]

Al igual que otras instituciones, la ciudadanía digital presenta limitaciones y problemas, asociados especialmente con la competencia de los ciudadanos para manejar información que les permita realizar el ejercicio ciudadano en un espacio virtual.

III. **Ideas Finales**

Las TIC han impactado en todos los ámbitos de la vida social, han redefinido instituciones clásicas y han permitido el surgimiento de nuevas; la política no ha sido impermeable a esta influencia, pudiendo hablarse en los tiempos actuales de nuevas formas de comportamiento político, de participación democrática y en definitiva de una nueva democracia en el entorno digital.

La idea de una ciudadanía digital deriva de una realidad evidente, relativa a las nuevas formas de ejercicio de la ciudadanía, en un espacio diferente al analógico: el virtual. Pero esta figura emergente precisa de

[21] Hay que considerar, como dice Robles, que "el uso de las TIC no es, de por sí, una causa directa de la desigualdad. El hecho de que unos ciudadanos y no otros utilicen, por ejemplo, Internet no es causa de asimetría social. Desde aquí, la vertiente desigualitaria del uso de las TIC presenta un carácter peculiar, a saber su naturaleza indirecta." Robles, José Manuel, Ob. Cit. Pág.

elementos y condiciones para su existencia, especialmente relacionados con el funcionamiento de Internet, sus aplicaciones y la regulación de los mismos, así como el comportamiento de los individuos frente a éstas.

La ciudadanía digital afronta importantes desafíos, que podrían incluso condicionar su legitimidad, como son: la brecha digital, el reconocimiento y legalización del uso de medios tecnológicos para el ejercicio ciudadano. Por su parte los ciudadanos digitales precisan de ciertos elementos para entenderse como tales, pues se consideran como condiciones básicas para atribuir tal condición, siendo la más importante la competencia en el manejo de información o alfabetización informacional, que deriva del nivel de educación de cada individuo y la percepción de utilidad de las herramientas informáticas para las actividades políticas y de relacionamiento con la administración pública.

REFERENCIAS:

Castells, Manuel, La galaxia Internet, Arete, Barcelona, 2001.

Mcluhan, Marshall, & Power, B.R., La aldea global, Gedisa, Barcelona, 1995. Traducción de Gilles Multigner. Versión digital disponible en http://www.ebiblioteca.org/?/ver/47142

Ribble, Mike, Bailey Gerald, y Ross Tweed, "Digital Citizenship, addressing aprópiate technology behavior", publicado en los números 1 y 2 del Volumen 32 de la revista Learning & Leading with Technology (http://www.iste.org/LL/32/1/index.cfm). Traducción realizada por Eduteka, versión en español disponible en: http://www.eduteka.org/CiudadaniaDigital.php

Robles, José Manuel, Ciudadanía Digital, Editorial UOC, Barcelona, España, 2011.

Sitios web consultados:

www.observatoriociudadaniadigital.org

www.eduteka.org

http://www.gobiernoelectronico.gob.ec/PlanGobiernoElectronicoV1.pdf

LA VENGANZA PORNOGRAFICA (REVENGE PORN) Y LA VIOLENCIA DE GENERO PERPESPECTIVAS DEL ORDENAMIENTO JURIDICO NORTEAMERICANO Y PUERTORRIQUEÑO

FREDRICK VEGA LOZADA, Catedrático Adjunto Facultad de Derecho Universidad Interamericana de Puerto Rico y Decano de la Facultad de Ciencias Económicas y Administrativas, fvega@intermetro.edu

Introducción

La Violencia de Genero es uno de los vestigios más denigrantes y despectivos de la Raza Humana1. En Costa Rica nuestros pueblos firmaron la Declaración Americana de Derechos Humanos que en sus Artículos 5 y 11 aspiran a prohibir la discriminación de Género y proteger la dignidad humana. Sin embargo, la violencia de genero especialmente contra las Mujeres ha tenido un nuevo impulso y devenir con el uso de las nuevas tecnologías, especialmente en las redes sociales El propósito de esta investigación es analizar un enfoque jurídico a la violación de los derechos humanos de la Venganza Pornográfica (Porn Revenge) y realizar un recorrido por las respuestas jurídicas en defensa del Bien jurídico

1 . Declaración Americana de Derechos Humanos, que dispuso que desde el 1942 el compromiso que los pueblos asumieron al fundar las Naciones Unidas en San Francisco (Estados Unidos), en 1942 la Carta de las Naciones Unidas menciona los derechos humanos en siete lugares de su texto expresamente. El quinto Considerando expresa claramente “que los pueblos de las Naciones Unidas han reafirmado en la Carta su fe en los derechos fundamentales del hombre, en la dignidad y el valor de la persona humana y en la igualdad de derechos de hombres y mujeres, y se han declarado resueltos a promover el progreso social y a elevar el nivel de vida dentro de un concepto más amplio de la libertad. Consejo de Derechos Humanos también debe cumplir con su papel de acuerdo con su mandato de "promover el respeto universal por la protección de todos los derechos humanos y libertades fundamentales de todas las personas, sin distinción de ningún tipo, y de una manera justa y equitativa" (GA 60/251, OP 2); La Declaración sobre la Eliminación de la Violencia contra la Mujer de la Asamblea General de las Naciones Unidas define como violencia de género: “Todo acto

de violencia basado en la pertenencia al sexo femenino que tenga o pueda tener como resultado un daño o sufrimiento físico, sexual o psicológico para la mujer, inclusive las amenazas o tales actos, la coacción o privación arbitraria, tanto si se producen en la vida pública o privada". 2. “Toda persona tiene derecho a que se respete su integridad física, psíquica y mora”1. “Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.”

de la Dignidad Humana y la igualdad de géneros en el Derecho Civil y Penal de distintos Estados de los Estados Unidos de Norteamérica (EUA) y del Estado Libre Asociado de Puerto Rico.

La Venganza Pornográfica (Revenge Porn)

Tan reciente como el 30 de julio de 2014 en la Corte de Primera Instancia de Houston ciudad del estado de Texas en el sur de EUA la empresa Facebook fue demandada por daños por la cantidad de 123 millones de dólares. La demanda alega que Facebook fue negligente al no tomar acción en contra del “Revenge porn” (La “pornografía de venganza”). La parte demandada alego que Facebook al no corregir en un tiempo razonable la información falsa y libelosa, de naturaleza sexual sobre la demandante causó a la parte demandante graves daños emocionales tanto a ella como a sus familiares.

Se le llama “Revenge porn” (La “pornografía de venganza”) a la pesadilla que cientos de mujeres en el mundo sufren debido a despechados de un ex novio que comparten fotos de ellas en poses eróticas o situaciones sexuales sin el permiso de la mujer2. Es una dura lección que cientos de mujeres han aprendido con sudor y lágrimas alrededor del mundo, ningún país no ha estado exento de casos en que una mujer ve vulnerada su privacidad, de una de las formas más humillantes, como lo es el ser exhibida totalmente desnuda ante

los ojos de curiosos de la web. Algunas mujeres han expresado en sus reclamaciones legales que “Es la denigración total como

2 . En EUA la definición generalizada es de Revenge Porn es “is the posting of nude or sexually explicit photographs or videos of people online without their consent, even if the photograph itself was taken with consent. A spurned spouse, girlfriend or boyfriend may get revenge by uploading photographs to websites, many of which are set up specifically for these kinds of photos or videos. The victim’s name, address and links to social media profiles are often included with the images, and some websites charge a fee to have the materials removed”. State 'Revenge Porn' Legislation. (Recuperado el 20 de Julio de 2014.) http://www.ncsl.org/research/telecommunications-and- information-technology/state-revenge-porn-legislation.aspx

La venganza pornográfica y la violencia de genero perspectivas del ordenamiento jurídico norteamericano y puertorriqueño Fredrick Vega-Lozada fvega@intermetro.edu Página 3 de 15

mujer”3. El primer país que comenzó la discusión legal sobre el tema fue en el Reino Unido4, cuando exparejas masculinos comenzaron a enviar a distintos portales pornográficos Videos o fotos de sus exparejas femeninas. Esta conducta se comenzó a realizar en los Estados Unidos y en otros países.

Veamos si el compartir fotografías eróticas y grabar videos sexuales con una pareja y que esta después lo envíe y publique sin permiso constituye una violencia contra la mujer La definición de las Naciones Unidas sobre Violencia sobre la Mujer la define en su versión en Inglés como: “violence directed at a woman because she is a woman or acts of violence which are suffered disproportionately by women”5. La violencia contra la mujer es una forma de discriminación y una violación de los derechos humanos. Causa sufrimientos indecibles, cercena vidas y deja a incontables mujeres viviendo con dolor y temor en todos los países del mundo. Causa perjuicio a las familias durante generaciones,

Empobrece a las comunidades y refuerza otras formas de violencia en las sociedades. La violencia contra la mujer pasó del plano privado al dominio público y al ámbito de responsabilidad de los Estados, en gran medida,

3 . “Revenge porn”: La pesadilla de sacarte fotos desnuda. (Recuperada el 27 de julio de 2014)http://tenareshi.com/index.php?option=com_content&view=article&id=572:revenge-porn-la-pesadilla-de- sacarte-fotos-desnuda&catid=45&Itemid=591, http://www.xojane.com/list/revenge-porn, Facebook “revenge porn” lawsuit hits Mark Zuckerberg where it hurts. Leonard , A (Recuperada el 30 de julio de 2014).http://www.salon.com/2014/07/30/facebook_revenge_porn_lawsuit_hits_mark_zuckerberg_where_it_hurts/

4 . New Technology: Same Old Problems. Report of a roundtable on social media and violence against women and girls co-hosted by the End Violence against Women Coalition and The Guardian July 2013. En las Recomendaciones Generales No. 19 (Sesión 11ava , 1992) .La definición de las Naciones Unidas sobre Violencia sobre la Mujer la define en su versión en Inglés como aquella “violence directed at a woman because she is a woman or acts of violence which are suffered disproportionately by women”

5 . Committee on the Elimination of Discrimination against Women general recommendation No. 19; Human Rights Committee, general comment 28; and Committee on Economic, Social and Cultural Rights general comment 16, in: HRI/GEN/1/Rev. 8. Véase, Committee on the Elimination of Discrimination against Women general recommendation. No. 19; Committee on the Elimination of Racial Discrimination, general recommendation 25. See note 24.

debido a la labor de base de las organizaciones y movimientos de mujeres en todo el mundo6. Las raíces de la violencia contra la mujer están en la desigualdad histórica de las relaciones de poder entre el hombre y la mujer y la discriminación generalizada contra la mujer en los sectores tanto público como privado. La forma más común de violencia experimentada por la mujer en todo el mundo es la violencia ejercida por su pareja en la intimidad, que a veces culmina en su muerte.

Las disparidades patriarcales de poder, las normas culturales discriminatorias y las desigualdades económicas se han utilizado para negar los derechos humanos de la mujer y perpetuar la violencia7. La violencia contra la mujer es uno de los principales medios que permiten al hombre mantener su control sobre la capacidad de acción y la sexualidad de la mujer. En el amplio contexto de la subordinación de la mujer, los factores concretos que causan la violencia son el uso de la fuerza para resolver conflictos, las doctrinas sobre la intimidad y la inercia de los Estados. Existen muchas formas diferentes de violencia contra la mujer: física, sexual, psicológica y económica8. Algunas cobran más importancia, mientras que otras las van perdiendo a medida que las sociedades experimentan cambios demográficos, reestructuración económica y transformaciones sociales y culturales. Las nuevas tecnologías pueden generar nuevas formas de violencia, como el acoso por internet o por

6 . Naciones Unidas. (2006) Poner fin a la violencia contra la mujer De las palabras los hechos. División para el Adelanto de la Mujer del Departamento de Asuntos Económicos y Sociales de la Secretaría de las Naciones Unidas. 7 . Sen, P., "Successes and Challenges: Understanding the Global Movement to End Violence Against Women in Global Civil Society", Kaldor, M., Anheier, H. and Glasius, M.,eds. (London, Centre for the Study of Global Governance, 2003); Reilly, N. ed., Without Reservation: The Beijing Tribunal on Accountability for Women's Human Rights (New Jersey, Center for Women's Global Leadership, 1996); and Jain, D., Women, Development, and the UN: A Sixty Year Quest for Equality and Justice (Bloomington, Indiana University Press, (2005).

8 . Ramiro, L., Hassan, F. and Peedicayil, A., "Risk markers of severe psychological violence against women: a WorldSAFE multi-country study", Injury Control and Safety Promotion, vol. 11, No. 2 (June 2004), pp. 131-137.

teléfonos móviles9. Por estas razones entendemos que el Revenge Porn o venganza Pornográfica es una forma de violencia de género, psicológica y sexual contra la mujer. Ahora que alternativas legales tiene la mujer que ha

sido víctima de este ultraje a su dignidad. Ordenamiento Jurídico de Estados Unidos de América Reclamaciones en el plano Civil Una de los tópicos más importantes para indemnizar los daños que puedan sufrir las mujeres de parte de sus exparejas y de las empresas que activamente o pasivamente participan en la acción o conducta dolosa o negligentemente en este tema de las posibles reclamaciones legales en el ámbito civil. La alternativa principal son las demandas en daños. Ahora en el ordenamiento jurídico norteamericano existe varios escollos jurídicos para uno de ellos es la existencia de la Sección 230 del Título V de la ley de Telecomunicaciones de 1996 y comúnmente conocida como la Ley de Decencia en las Comunicaciones10. La política pública de esta ley dispone cuyos objetivos son: "(1) promover el desarrollo continuo de la Internet y otros servicios informáticos interactivos y otros medios interactivos; (2) para preservar el libre mercado dinámico y competitivo que existe actualmente para la Internet y otros servicios informáticos interactivos, libre de regulación estatal o federal; (3) fomentar el desarrollo de tecnologías que maximizan el control del usuario sobre la información que es recibida por los individuos, familias y escuelas que utilizan el Internet y otros servicios informáticos interactivos; (4) para eliminar los desincentivos para el desarrollo y la utilización de bloqueo y filtrado de tecnologías que permiten a los padres restringir el acceso de sus hijos en línea a material objetable o inapropiado, y

9 . Ibíd., 2. 10 . 47 U.S.C. § 230

(5) para garantizar la observancia estricta de las leyes penales federales para disuadir y sancionar la trata de obscenidad, acoso y el acoso por medio de la computadora11.

En particular, la Sección 230 de la Ley fue promulgada para asegurar que los proveedores y usuarios de "servicios de informática" no estarían expuestos a la responsabilidad como "editores de contenido" de cualquier información proporcionada por otro "proveedor de información de contenido.12" La Sección 230 de la Ley de Decencia en las Comunicaciones dispone que "ningún

proveedor o usuario de un servicio informático interactivo será tratado como el editor o representante de cualquier información proporcionada por otro proveedor de contenido de la información.13"

La ley define "servicio informático interactivo" como "cualquier servicio de información, sistema o proveedor de software de acceso que proporciona o permite acceso a una computadora por varios usuarios a un servidor de la computadora, incluyendo específicamente un servicio o sistema que proporciona acceso a Internet y tales sistemas operados o servicios ofrecidos por las bibliotecas o centros de enseñanza. "14 "Proveedor de contenido de la información" se define como "cualquier persona o entidad que es responsable, en todo o en parte, por la creación o el desarrollo de la información proporcionada a través de Internet o cualquier otro". 15 Entonces quiere decir que bajo las inmunidades dispuesta por esta ley de 1996 los proveedores de servicios de Internet no serán responsables por lo que exponga en el servicio de Internet solamente

11 . 47 USC 230 (b). 12 . H. R. Rep. N º 105-775 ยง I (E).

13 . 47 USC 230 (c) (1). 14 . 47 USC ยง 230 (f) (2). 15 . 47 USC ยง 230 (f) (3)...

responderá el tercero, quien hizo la expresión sea cual fuera, por lo que los proveedores de Internet que por la amplitud de las definiciones de la Sección 230 incluyen en la actualidad a las redes sociales no son responsable civilmente16. Sin embargo, la ley dispone de excepciones importantes para apoderar a las víctimas del Revenge Porn. Para que estas puedan puedan acceder a reclamar indemnización contra las empresas proveedoras de Servicios de Internet incluidas las redes sociales estas excepciones son

16 . Zeran v. America Online, Inc. – La Corte de Apelaciones de EE.UU. para el Cuarto Circuito que evaluó la dirección del alcance de la de inmunidad de la Sección 230, en Zeran contra America Online, Inc., 129 F. 3d 327, 330 (4th Cir. 1997). En ese caso, el demandante demandó

a America Online, Inc., por no eliminar los mensajes difamatorios publicados por un tercero identificado, negándose a publicar retractaciones de los mensajes, y el negarse a impedir el acceso a la pantalla de anuncios similares después de haber sido informado del carácter difamatorio de los mensajes publicados. Al confirmar la desestimación de las alegaciones del demandante, el Cuarto Circuito señaló que en la promulgación de la Sección 230 "Congress recognized the threat that tort-based lawsuits post to freedom of speech in the new and burgeoning Internet medium "y el propósito de "encourage service providers to self-regulate the dissemination of offensive material over their services." Zeran, 129 F.3d at 330-331.El Tribunal rechazó específicamente el alegato de Zeran en cuanto a que la sección 230 elimina la responsabilidad editorial, dejando la responsabilidad de los distribuidores de material difamatorio intactos, sosteniendo que la responsabilidad del distribuidor era "merely a subset, or species, of publisher liability, and is therefore also foreclosed by § 230." Aunque la decisión de Zeran es a menudo exagerado por proporcionar inmunidad a un ICS para cualquier reclamación que surja de los contenidos de terceros, el Cuarto Circuito establece claramente que el artículo 230 "precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions--such as deciding whether to publish, withdraw, postpone or alter content- -are barred." Zeran, 129 F.3d at 330. Los Tribunales al interpretar la Sección 230 han seguido generalmente el análisis de Zeran. Véase, por ejemplo, Green v. America Online, 318 F.3d 465, 470-71 (3d Cir. 2003),Batzel v. Smith, 333 F.3d 1018, 1031 n. 18 (9th Cir. 2003), Carafano v. Metrosplash.com Inc., 339 F.3d 1119, 1122 (9th Cir. 2003), Ben Ezra, Weinstein & Co. v. America Online Inc., 206 F.3d 980, 984-86 (10th Cir. 2000)

En Doe vs MySpace, 474 F. Supp .2 d 843, 848 (WD Tex 2007), una madre de un usuario de MySpace menor de edad presentó una demanda contra el propietario del sitio web y el operador después de que el menor fue asaltado sexualmente por un hombre que se reunió a través del sitio de redes sociales. El tribunal aplicó Zeran, por analogías las alegaciones del demandante que MySpace sabía que habían depredadores sexuales y que usaban el servicio para comunicarse con los menores y de no reaccionar de forma apropiada con

las reclamaciones. El tribunal interpretó el artículo 230 de inmunidad general, al considerar que el tribunal sostuvo que MySpace tenía derecho a la inmunidad en virtud de la Ley de Decencia en las Comunicaciones. La mayoría de los circuitos aplican Zeran y la Sección 230 (c) (1) siempre que los Proveedores se abstengan de la filtración o censurar la información en sus sitios. Ver Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1322 n.3 (Cir 11 de 2006). Sin embargo, el Séptimo Circuito ha llamado recientemente la celebración de Zeran en tela de juicio al concluir que la Ley de Decencia en las Comunicaciones no es necesariamente inconsistente con las leyes estatales que genera la responsabilidad de los proveedores de ICS que se abstengan de filtrar o censurar el contenido.

Ver a Doe v. GTE Corp., 347 F. 3d 655, 660 (7th Cir. 2003). En dicta, el tribunal Pérez cuestionó la dependencia de los demás tribunales sobre Zeran: "If this reading [from Zeran, Ben Ezra, Green, and Batzel] is sound, then § 230(c) as a whole makes ISPs indifferent to the content of information they host or transmit: whether they do (§ (c)(2)) or do not (§ (c)(1)) take precautions, there is no liability under either state or federal law. As precautions are costly, not only in direct outlay but also in lost revenue from the filtered customers, ISPs may be expected to take the do-nothing option and enjoy immunity under § 230(c)(1). Yet § 230(c) - which is, recall, part of the "CDA" - bears the title "Protection for 'Good Samaritan' blocking and screening of offensive material", hardly an apt description if its principal effect is to induce ISPs to do nothing about the distribution of indecent and offensive materials via their services. Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?"

desconocidas pero muy útiles para lograr prevalecer en una reclamación legal en una corte de justicia.

Las excepciones a la inmunidad de la Sección 230 y el campo ocupado

En particular, el Estatuto establece que "no se interpretará en menoscabo del cumplimiento" de alguna de las leyes penales federales o "para limitar o ampliar cualquier legislación relativa a la propiedad intelectual."17 Esta excepción relacionada con la propiedad intelectual específicamente con el derecho de autor es muy importante en términos del Revenge Porn porque a quien pertenece el derecho de autor de las fotos o imágenes o sonido que se envía al recipiente mi expareja o a quien las envía. Entonces se podría alegar que se viola mi derecho de autor sobre las fotos al publicarlas por internet sin mi consentimiento expreso. Esto derrumbaría entonces la Inmunidad de la sección 230. Además, el artículo 230 promueve el cumplimiento de cualquier ley estatal coherente con " la aplicación de la Electronic Communications Privacy Act (ECPA)18 de 198619 o cualquiera de las modificaciones introducidas por dicha Ley20, o cualquier ley estatal similar." 21

17 . 47 USC ยง 230 (e) (1) y (2). 18 . (1) No effect on criminal law Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.(2) No effect on intellectual property law Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.(3) State law Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section. (4) No effect on communications privacy law Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law. 19 . "The ECPA defines [the term] 'electronic communication' as 'any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectric, or photocell system that affects interstate commerce”. Las Redes Sociales los Portales, Blogs y correo-e e protegido por esta ley , "the legislative history clearly shows Congress' intent to include it within the definition of 'electronic communications.'" 20 . La Ley Electronic Communications Privacy Act of 1986

(ECPA). (18 U.S.C. § 2701-11) "prohibits the intentional or willful interception, accession, disclosure, or use of one's electronic communication."

La venganza pornográfica y la violencia de genero perspectivas del ordenamiento jurídico norteamericano y puertorriqueño Fredrick Vega-Lozada fvega@intermetro.edu Página 9 de 15

Es importante destacar la prohibición a la divulgación que nos trae la ley de ECPA la Ley Electronic Communications Privacy Act of 1986 (ECPA). (18 U.S.C. § 2701-11) en cuanto a prohibir la divulgación, "prohibits the intentional or willful interception, accession, disclosure, or use of one's electronic communication.” Otra excepción vital poco comentada, que las fotos que se toman y se las transmite a mi pareja para su uso y satisfacción no pueden ser divulgadas posteriormente a terceros sin el consentimiento de la entonces expareja. Es que no se puede divulgar esta imagen. La excepción que dispone la Ley será si hay consentimiento. Ahora bien, la foto de mi cuerpo desnudo al yo enviársela a mi pareja constituye un consentimiento para que esta su vez la envié a un tercero cuando ya no seamos pareja. Pues es, nuestra hipótesis que sí no hay consentimiento informado que es obviamente un consentimiento para compartir es una violación a esta ley y a otras leyes estatales. Por ejemplo, en el caso de Robbins v. Lower Merion School District (2010)22, conocido como el caso de los "WebcamGate", llegó a una estipulación por cerca de $610,000 dólares porque dos escuelas superiores (bachillerato) probaron que habían violado las disposiciones de ECPA al activar remotamente en una laptops que habían distribuidos a sus estudiantes cerca de 66,000 “webshots” y “screenshots”. Incluyendo fotos del “webcam” en las habitaciones de los estudiantes y que fueron sustraídas por las Escuelas quienes eran dueños de las laptops o computadoras personales. Quiere decir que no importa que yo consentí y sabía que el equipo era de mi escuela y que me lo había provisto para producir mi tarea académica yo

21 . 47 USC ยง 230 (e) (3) y (4). 22 . In the Matter of LOWER MERION SCHOOL DISTRICT, Appellant, v. BLAKE J. ROBBINS, HANSON COURT March 9, 2012, Filed Appeal from the United States District Court for the Eastern District of Pennsylvania. Date filed: February 23, 2010. Barnes v. Yahoo!, Inc., 2005 WL

3005602, (D. Or. 2005) este es un caso interesante y emblemático sobre el tema.

tenía una clara expectativa a mi privacidad, y la Escuela violo mi derecho a la privacidad al tener acceso a esas fotos aunque con las fotos que me tomen con esas cámaras que me fueron provistas por mi escuela. Claro en este caso, había un interés del Estado porque eran menores los involucrados.

La Relación Contractual como Causa Próxima del Daño

Las relaciones Contractuales permea la proliferación de la impunidad de las conductas relacionadas al Revenge Porn y es que en todos los portales y redes sociales hay contratos de uso explícitos23. Por lo tanto, ¿qué ocurre cuando yo le aviso a mi Red Social que me han llevado mis fotos o que han construido con mis fotos un perfil ficticio e inexistente y que en este perfil se están publicando fotos trabajadas o cambiadas por una aplicación común como "Photoshop" y esta imagen mancilla mi integridad? Bueno ya sabemos que la Red Social esta exenta de responsabilidad por la Sección CDA 230 pero a su vez, la ley misma sección 230 (c) (2) le da la protección de Buen Samaritano a la Red Social cuando hay una expresión en la ley que a su mejor entendido: "c) Protection for "Good Samaritan" blocking and screening of offensive material (1) Treatment of publisher or speaker No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (2) Civil liability No provider or user of an interactive computer service shall be held liable on account of— (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy,

23 . Doe v. MySpace, 528 F.3d 413 (5th Cir. 2008)

excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)" Por lo tanto, si yo soy objeto de Revenge Porn y le advierto a la Red Social a la cual yo soy cliente que soy objeto de esta vejamen a mi dignidad y la Red Social no hace nada sabiendo que esta inmune y que aplica la sección del buen Samaritano pero no hace nada, esto constituiría una violación del contrato de servicio entre la Red y el usuario y por lo tanto una negligencia de la Red Social y en la causa próxima del daño. Es una alternativa aunque reconocemos que es un argumento legal débil. La Protección Jurídica Criminal El estado de California fue el primero en legislar en contra de la conducta del revenge porn en EUA. En la actualidad hay 10 estados24 en los EUA que reglamentan en el ámbito penal esta conducta. El estado de Arizona25 tiene la legislación más estricta aplicable a esta conducta dispone que el divulgar información sin el consentimiento puede ser considerado un delito grave con penas de reclusión de más de 1 año26. Los demás estados lo consideran un delito de menor grado que acarrea penas de menos de un año27. La mayoría de las legislaciones estatales aprobadas contiene unas excepciones para su aplicación para tratar de armonizar la ley con las excepciones Constitucionales de EUA y su Primera Enmienda de libertad de expresión.

24 . Arizona, Colorado, Georgia, Hawaii, Idaho, Maryland, Pennsylvania, Utah, Virginia y Wisconsin. Es prudente recalcar que en los estados de Alaska, Texas y New Jersey hay leyes que regulan esta conducta del Revenge Porn pero que no están bajo esos títulos, en el estado de New Jersey hay ya tres convicciones de ciudadanos por este tipo de conducta del revenge porn pero bajo la legislación del Privacidad en las comunicaciones. 25 . Title 13, Chapter 14, Arizona Revised Statutes (A.R.S.), A.R.S. § 13-1424Arizona Law HB2515 unlawful distribution of private images 26 . "Prohibits a person from knowingly disclosing, displaying, distributing, publishing, advertising or offering a photograph, videotape or film or digital recording or other reproduction of a person engaged in a sexual act or in a state of nudity without that person's written consent". Ibíd, 24.

27 . En el ordenamiento jurídico probatorio norteamericano le ofrece al cuerpo del ministerio público o Fiscalía más recursos probatorios cuando son considerados los delitos de mayor grado.

La venganza pornográfica y la violencia de genero perspectivas del ordenamiento jurídico norteamericano y puertorriqueño Fredrick Vega-Lozada fvega@intermetro.edu Página 12 de 15

Por ejemplo, la ley no aplica a imágenes que se divulgan para: el beneficio del interés público, por las autoridades del estado en sus investigaciones criminales o administrativas bona fides o por el tratamiento médico. Ahora la ley de Arizona que entro en vigor el 1ero de mayo de 2014 contiene una excepción innovadora como es la de "images involving voluntary exposure in a public or commercial setting.28" Esto hace que esta legislación sea diferente porque reconoce la pornografía no consensual como un delito de obscenidad esta es una corriente innovadora en EUA porque en las 9 legislaciones estales se considera que la conducta del revenge porn es un acoso, una invasión a la privacidad o una conducta de inclusive de alteración de la paz (disorderly conduct)29. Diferente a otras legislaciones penales sobre el tema en Arizona no se requiere prueba de la intención para causar estrés, desasosiego o daño en la victima. Esto también es un paso de protección adicional que es distinto e innovador hay Comentaristas en las Facultades de Derecho norteamericanas que concluyen que la conducta del revenge porn no es precisamente por la venganza sino que es por ganar dinero o ganar popularidad y el daño real a la víctima es precisamente la divulgación de la imágenes o sonido no consentido de la expareja y no debería entonces haber más prueba sobre la intención de la conducta. Puerto Rico En Puerto Rico, La Constitución en su Artículo II de la Carta de Derechos dispone la Protección a la mujer y al derecho a la privacidad es un bien jurídico de la más alta protección por todo el ordenamiento30. En materia

28 . "Exempts the following from the above prohibition: 1. Lawful and common practices of law enforcement, reporting criminal activity to law enforcement, or when permitted or required by law or rule in legal proceedings. 2. Medical treatment. 3 Images involving voluntary exposure in a public or commercial setting". Ibíd., 24. 29 . Teicher Khadaroo, S. Revenge porn: With Arizona, 10 states now outlaw such postings. May 1,

2014. (Recuperado el 25 de julio de 2014). http://www.csmonitor.com/USA/Politics/2014/0501/Revenge-porn-With-Arizona-10-states-now-outlaw-such-postings 30 . Sección 1. La dignidad del ser humano es inviolable. Todos los hombres son iguales ante la Ley. No podrá establecerse discrimen alguno por motivo de raza, color, sexo, nacimiento, origen o condición social, ni ideas

civil proceden las demandas en daños para indemnizar a las víctimas. Sin embargo, lograr una protección sobre el asunto en materia penal está expresamente contenidos en el Código Penal igual que como ocurre en algunos estados como Nueva Jersey, en Puerto Rico se siguió el concepto de invasión a la privacidad. Para proteger a las víctimas de atentados contra el honor en el Artículo 173 del Código Penal de Puerto Rico de 2012 se dispone sobre la Revelación de comunicaciones y datos personales31. En Puerto Rico, la protección relativa a conductas como el Revenge Porn va entorno a los delitos sobre la invasión a la Privacidad32 en el caso de que sea una menor la

políticas o religiosas. Y en la Sección 8. Toda persona tiene derecho a protección de ley contra ataques abusivos a su honra, a su reputación y a su vida privada o familiar. 31 . “Toda persona que difunda, publique, revele o ceda a un tercero los datos, comunicaciones o hechos descubiertos o las imágenes captadas a que se refieren los Artículos 171 (Violación de comunicaciones personales) y 172 (Alteración y uso de datos personales en archivos), o que estableciere una empresa para distribuir o proveer acceso a información obtenida por otras personas en violación de los referidos Artículos, u ofreciere o solicitare tal distribución o acceso será sancionada con pena de reclusión por un término fijo de tres (3) años” Artículo 171.- Violación de comunicaciones personales. Toda persona que sin autorización, y con el propósito de enterarse o permitir que cualquiera otra se entere, se apodere de los papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos de otra persona, o intercepte sus telecomunicaciones a través de cualquier medio, o sustraiga o permita sustraer los registros o récords de

comunicaciones, remesas o correspondencias cursadas a través de entidades que provean esos servicios, o utilice aparatos o mecanismos técnicos de escucha, transmisión, grabación o reproducción del texto, sonido, imagen, o de cualquier otra señal de comunicación, o altere su contenido será sancionada con pena de reclusión por un término fijo de tres (3) años. A los fines de este Artículo, el hecho de que la persona tuviere acceso a los documentos, efectos o comunicaciones a que se hace referencia dentro de sus funciones oficiales de trabajo no constituirá de por sí "autorización" a enterarse o hacer uso de la información más allá de sus estrictas funciones de trabajo. El Artículo 172.- Alteración y uso de datos personales en archivos. Toda persona que, sin estar autorizada, se apodere, utilice, modifique o altere, en perjuicio del titular de los datos o de un tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en discos o archivos informáticos o electrónicos, o en cualquier otro tipo de archivo o registro público o privado, será sancionada con pena de reclusión por un término fijo de tres (3) años. Artículo 175.- Delito agravado, Si los delitos que se tipifican en los Artículos 171 (Violación de comunicaciones personales), 172 (Alteración y uso de datos personales en archivos) y 173 (Revelación de comunicaciones y datos personales), se realizan con propósito de lucro por las personas encargadas o responsables de los discos o archivos informáticos, electrónicos o de cualquier otro tipo de archivos o registros; o por funcionarios o empleados en el curso de sus deberes será sancionada con pena de reclusión por un término fijo de ocho (8) años". 32 . Lozada Tirado v. Tirado Flecha, 2010 T.S.P.R. 9; Aponte Hernandez v. Sánchez Ramos I, 2008 T.S.P.R. 53; Umpierre Biascoechea v. Banco Popular, 170 D.P.R. 205, 212 n. 4 (2007); Id. en la pág. 234; Hernández Vélez v. Televicentro, 168 D.P.R. 803, 837 (2006); Delgado, ex parte, 165 D.P.R. 170 (2005); Serrano, Vélez v. E.L.A., 154 D.P.R. 418 (2001) Andino Torres, ex parte, 151 D.P.R. 794, 806-807 (2000); Pres. del Senado, 148 D.P.R. 737 (1999); Arroyo v. Rattan Specialties, Inc., 117 D.P.R. 35 (1986); Green Giant Co. v. Tribunal Superior, 104 D.P.R. 489 (1975); Figueroa v. Díaz, 75 D.P.R.163 (1953). También hay unos excelentes artículos en donde el derecho de la Dignidad humana son tratados en específico como uno independiente estos son: Hiram Meléndez Juarbe, Privacy in Puerto Rico and the Madman's Plight: Decisions, 9 Geo. J. Gen. & L. 1 (2008), Luis Aníbal Avilés Pagán, Human Dignity, Privacy and Personality Rights in the Constitutional

Jurisprudence of Germany, the United States and the Commonwealth of Puerto Rico, 67 Rev. Jurídica U.P.R. 343 (1998) y el discurso del insigne Profesor

agraviada por esta conducta sin protección jurídica seria encausado por los delitos relacionados a la pornografía infantil33. Específicamente en la ley para prevenir la Violencia Domestica34dispone como el atentado a la dignidad de la mujer lo actos de violencia y en esta amplitud este acto del Revenge Porn estaría tipificado. Conclusión En esta presentación hemos intentamos exponer las perspectivas norteamericanas sobre Revenge Porn, esta nueva forma de violencia en contra de la dignidad de la mujer en el mundo virtual y globalizado en la era de la información.

Concluimos que es un acto de violencia contra la mujer pero que en EUA salvo disposiciones específicas de naturaleza penal no hay muchas alternativas civiles para que la mujer agraviada pueda resarcir su daño de la conducta negligente de su expareja o de quien tuvo acceso a sus fotos íntimas. Esta por dilucidarse en los foros correspondientes el alcance de la

Constitucionalista Carlos E. Ramos González, Discurso, La inviolabilidad de la dignidad humana: Lo indigno de la búsqueda de expectativas razonables de intimidad en el derecho constitucional puertorriqueño (Facultad de Derecho de la Universidad Interamericana de Puerto Rico, San Juan, Puerto Rico, 28 de octubre de 2010). 33 . Artículos 143, 144, el artículo 147.- Posesión y distribución de pornografía infantil. “Toda persona que a sabiendas posea o compre material o un espectáculo de pornografía infantil será sancionada con pena de reclusión por un término fijo de doce (12) años. Toda persona que a sabiendas imprima, venda, exhiba, distribuya, publique, transmita, traspase, envíe o circule material o un espectáculo de pornografía infantil será sancionada con pena de reclusión por un término fijo de quince (15) años, el artículo 148.- Utilización de un menor para pornografía infantil. Toda persona que use, persuada o induzca a un menor a posar, modelar o ejecutar conducta sexual con el propósito de preparar, imprimir o exhibir material de pornografía

infantil o a participar en un espectáculo de esa naturaleza será sancionada con pena de reclusión por un término fijo de quince (15) años. Será sancionada con pena de reclusión por un término fijo de veinte (20) años: (a) cuando el acusado tenga relaciones de parentesco con la víctima, por ser ascendiente o descendiente, por consanguinidad, adopción o afinidad, hasta el tercer grado, o por compartir o poseer la custodia física o patria potestad; o (b) cuando se cometa en el hogar o lugar dedicado al cuidado de la víctima, artículo 152.- Transmisión o retransmisión de material obsceno o de pornografía infantil. Toda persona que a sabiendas distribuya cualquier material obsceno a través de cualquier medio de comunicación telemática u otro medio de comunicación, incurrirá en delito menos grave. Cuando el material sea de pornografía infantil, la persona será sancionada con pena de reclusión por un término fijo de ocho (8) años". 34 . Ley de Violencia Doméstica, Ley Núm. 54 del 15 de agosto de 1989, 8 L.P.R.A. §§ 601 et seq.

La venganza pornográfica y la violencia de genero perspectivas del ordenamiento jurídico norteamericano y puertorriqueño Fredrick Vega-Lozada fvega@intermetro.edu Página 15 de 15

legislación actual específica sobre el tema. Preguntas tales como: ¿Serán válidas las leyes estatales al enfrentarse a cuestionamientos de naturaleza Constitucional por enfrentar la 14ava Enmienda federal de Libertad de Expresión?

Planteamos dos alternativas viables actuales para lograr justicia en la mujer agraviada. Las excepciones a la inmunidad de la Sección 230 y tan bien nos parece que la legislación de protección a la privacidad puede resultar en una alternativa exitosa para resarcir los agravios de esta conducta. Por limitación del trabajo no hemos entrado en los problemas probatorios de demostrar el origen de los Revenge Porn35, ni la expresión anónima, ni las controversias asociadas al derecho a la imagen. Pero concluimos que aunque de no fácil solución legal, esta violencia contra la mujer que nos trae los adelantos tecnológicos está siendo atendida con premura por los ordenamientos jurídicos de EUA y Puerto Rico.

[i] En el año 1950 Ludwig von Bertalanffy, biólogo, propuso una teoría general de sistemas argumentando la naturaleza total que llamó "holística" de la organización de sistemas complejos. Ello motivó una extensa literatura y nuevas áreas de investigación caracterizadas por la búsqueda de respuesta a problemas complejos, desde la interdisciplinariedad y la complementariedad de enfoques a la hora de atender las distintas dimensiones del quehacer humano y sus postulados fueron incorporados a los estudios cibernéticos desde ese momento.

[ii] El "Proyecto Cibersin", fue diseñado para servir como el "sistema nervioso" de la economía chilena con el propósito de crear los lazos funcionales necesarios entre la CORFO, el gobierno y la sociedad. Proyecto de Investigación en homenaje a Stanford Beer y Salvador Allende. Yarina Amoroso Fernández. 2012-2014.

El cumplimiento a la ley federal de protección de datos personales en posesión de particulares, Oscar Flores, México

El cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, el caso de México. Propuestas para fortalecer a la autoridad administrativa encargada de la verificación.

El cinco de julio de dos mil diez en México despertamos con la grandiosa noticia de que existía ya en el derecho positivo un novedoso cuerpo normativo especializado en la protección de los datos personales, ahora se regularía la posesión de los mismos para el caso de los que poseyeran los particulares.

Dicha noticia sonaba por demás interesante, pues una regulación de tal envergadura nos colocaba a la altura de las grandes naciones, las más progresistas, las más novedosas, pero también las que mejor se dedican a las actividades comerciales en las que interfieren las transferencias de datos personales.

A partir de esa fecha se inauguró una nueva etapa del organismo descentralizado no sectorizado de la Administración Pública Federal mexicana, denominado Instituto Federal de Acceso a la Información Pública y a partir de entonces denominado, Instituto Federal de Acceso a la Información Pública y Protección de Datos.

De forma interna en el ámbito administrativo ese organismo vivió la adición de un apéndice, se le creó una nueva área especializada, una nueva Secretaría denominada, como es lógico, de protección de datos personales, para en ese

orden de ideas contar con 3 secretarías; una secretaría general dedicada a llevar la vida administrativa y organizacional del instituto, una secretaría de acceso a la información pública y una tercera de protección de datos personales.

Además de contar con una Dirección General de Asuntos Jurídicos, una Dirección General de Comunicación Social, la Secretaría Técnica del Pleno y su contraloría.

En esos términos se dio y se vivió este primer cambio normativo para el llamado IFAI, una autoridad de vanguardia y referencia en materia de transparencia, no sólo garante del ejercicio del derecho a la información, sino también de los archivos y la protección de datos en posesión de organismos públicos y a partir de ahí, también en la posesión de datos personales en posesión de particulares.

Desde esa fecha, tal vez desde un poco antes, se ha hablado mucho, la mayoría de las veces en términos positivos y aplaudiendo sobre esta nueva legislación, sobre este nuevo IFAI y sobre el cambio maravilloso que viviríamos en México deteniendo por fin esa voracidad en contra de la intimidad, la privacidad y sobre todo en beneficio de las personas, en beneficio de su información personal.

Hoy, al segundo semestre de 2014 puedo afirmar categóricamente que no ha sido así. Hemos hablando mucho en términos abstractos sobre la novedad normativa, sobre los intangibles beneficios, pero hemos hablado poco sobre la autoridad encargada y su actuación, salvo en pequeños casos donde los medios se han referido a algunos de los incipientes éxitos de la autoridad en esta materia.

Este trabajo ahondará en este tema, lo abordaremos en los siguientes términos; su impacto en la cultura ciudadana en beneficio de la concientización sobre los datos personales y su respeto, el impacto de la labor de verificación de la autoridad administrativa y por último, el número de procedimientos instaurados por esta autoridad en la materia.

La labor del IFAI en materia de protección de datos personales en posesión de particulares y su impacto en la cultura ciudadana.

La comunicación social es la labor a través de la cual los organismos e instituciones públicas difunden su función, sus actividades, sus planes y programas de acción, en beneficio del derecho a la información de la sociedad.

Una forma de ejercer la comunicación social es la denominada, a mi parecer malamente denominada, “publicidad oficial”, la cual podemos entender como una serie de acciones para entablar canales directos de comunicación entre el Estado, sus dependencias y entidades en sus tres niveles de gobierno y la

ciudadanía. Ésta, por su propia naturaleza y necesidad, tiene que ser clara, objetiva y entendible, por restricción constitucional, no debe promover a personas.

Su alcance y composición es global, comprende todas las acciones informativas y de difusión, a través de cualquier medio de comunicación; impreso, electrónico, digital (me atrevería a mencionar a la información en redes sociales cuando es contratada a alguna empresa especializada), siempre y cuando haya sido contratada o pagada por un ente público de cualquier orden de gobierno.

Esta forma de comunicación no tiene ninguna finalidad comercial, sino por el contrario es información generada por el gobierno, encaminada primordialmente a difundir mensajes a la sociedad, ya sean informativos o formativos. El fin trascendente de este tipo de acciones es, en parte, hacer efectivo el derecho a la información de las personas.

Muchos, lamentablemente muchos de los casos pasados y presentes de comunicación social han sido más conocidos por ser empleados por los gobernantes en turno para promover su imagen y, en su caso, ensalzar sus logros o pretender manipular la opinión pública. Un buen ejercicio de comunicación social debe estar más orientado a informar y formar a la

ciudadanía, cada uno de los órganos de los poderes públicos debiera formar e informar a la ciudadanía en su ámbito de especialidad.

Es al IFAI, principalmente al IFAI a quien le corresponde ejercer liderazgo en materia de formación e información sobre los datos personales, la concientización sobre su importancia y difundir una cultura de respeto y debido tratamiento.

Partamos de la idea de saber si el IFAI como órgano público está desarrollando labores de comunicación social, acciones de difusión o información sobre la protección de datos personales.

De una revisión al apartado de comunicación social de su portal institucional de internet, encontramos que entre enero y agosto de 2014 ese organismo ha publicado 50 boletines de prensa sobre su actividad; de los cuales menos de 10 están relacionados con la materia que nos ocupa, para el año 2013 el instituto publicó 139 boletines de prensa, de los cuales mucho menos de la mitad están relacionada, para el caso de 2012 el número de boletines de prensa fue de 173, de igual forma, menos de la mitad de ellos tienen que ver con el tema de interés.

Para 2011 la tendencia no cambia, se publicaron 182 boletines, pero el número de especializados en el tema no es significativo. El caso de 2010 para nada

revierte la tendencia; 165 boletines, pero ni siquiera la mitad sobre el tema de la protección de datos personales.

Pero por qué tanta importancia en este tema, porque es el boletín informativo uno de los principales productos informativos que emanan de un ente público, contiene la información esencial sobre un hecho, evento o acto público relacionado con el órgano emisor, en el caso del IFAI los más comunes son los relacionados con las sesiones públicas del pleno de sus comisionados, aquellas en donde se resuelven los asuntos sometidos a su jurisdicción.

Es decir, para el propio IFAI no ha sido de vital importancia resaltar el tratamiento de estos temas en las sesiones de resolución de su Pleno, sino, se ha ponderado históricamente los temas vinculados con el derecho de acceso a la información pública. Esto es entendible, en su joven vida, el IFAI se ha destacado como la autoridad en materia de transparencia, pero considero poco oportuno dar menos importancia al tratamiento de las resoluciones sobre protección de datos.

Actualmente existe poca información acerca del nivel de conocimiento que predomina sobre qué es la protección de datos personales en posesión de particulares, qué es el IFAI como autoridad reguladora y en general sobre la cultura de la protección de datos personales.

Pero dentro de esa poca información existe un par de valiosas mediciones, primero tenemos que la empresa “Parametría, Investigación estratégica, análisis de opinión y de mercado” en este 2014 la empresa encuestadora destaca que a pesar de la importancia que tiene el IFAI para la sociedad, es una institución poco conocida por los mexicanos, de acuerdo con sus propios datos el mes de mayo, el 72% de la población entrevistada no supo qué era o a qué se encargaba dicho organismo.

Apenas un 18% de la población refirió de forma correcta qué es el instituto. Aunque el estudio de parametria no lo trata, pero podemos inferir de forma lógica que entre los encuestados impera el mismo nivel de desconocimiento sobre la labor del IFAI como organismo garante de la protección de datos personales en posesión de los particulares.

El segundo de los estudios que me resulta sumamente revelador es el llevado a cabo por la AMIPCI, Asociación Mexicana de Internet, denominado “Primer Estudio sobre Protección de Datos Personales entre Usuarios y Empresas en México”, dicho estudio tuvo una doble dirección, fue aplicado a representantes de empresas, así como a personas. Revisemos los resultados.

En el apartado de empresas tenemos que el 44% de los encuestados respondieron no tener conocimientos necesarios sobre qué es la Ley Federal de Protección de Datos Personales en Posesión de Particulares, por otro lado,

3 de cada 10 no sabe cómo se debe dar cumplimiento a la referida Ley. Para cerrar este rubro, el 74% de los encuestados coincidieron en que no existe la difusión necesaria sobre la Ley y la autoridad encargada de su cumplimiento.

¿Pero qué pasa con las personas? Veámoslo a continuación, según el mismo estudio de la AMIPCI, más del 30% de la población encuestada no sabe qué es un dato personal.

De este par de referencia de conocimiento de la población es fácil concluir que no existe una suficiente y eficiente difusión de la información sobre la cultura de protección de datos personales en posesión de particular, el IFAI como la autoridad encargada de su protección, así como de la Ley de la materia.

La labor de verificación administrativa y la función jurisdiccional del IFAI.

Hasta ahora hemos analizado el actuar no jurisdiccional del IFAI, es decir esa función de difusor y propagador de una cultura, pero ahora veamos de cerca qué pasa con el cumplimiento de su función primordial.

La importancia de los procedimientos administrativos y más aún, de las resoluciones a esos procedimientos no es la imposición o no de una sanción, sino el antecedente que se genera, los argumentos que en el pleno durante la discusión, el rico intercambio de ideas que debe generarse en el análisis.

De esta suerte, no sólo se genera una sanción o no, sino se fija un antecedente que abre brecha en la materia y no hay alguien más que deba hacerlo, que no sea el propio IFAI.

Revisemos ahora cómo ha sido la productividad de su función jurisdiccional. Según la página de internet del propio instituto, en lo que va de este año se han emitido solamente 34 resoluciones administrativos, de las cuales únicamente en dos se ha impuesto una sanción al sujeto regulado, el resto fueron publicadas con sobreseimientos y desecamientos.

El antecedente para 2013 no es muy diferente, en todo ese año el Instituto emitió únicamente 67 resoluciones, en ese ejercicio hubo 27 resoluciones con sanción, el resto fueron desecamientos y sobreseimientos también.

Para 2012, el panorama es más complicado, pues únicamente se emitieron 27 resoluciones y solamente se sancionó en 4 de ellos.

Para 2011 únicamente se emitió una resolución. Sin duda, es poca la actividad jurisdiccional en la materia, al destacar que existen pocas sanciones no asevero, ni muchos, sostengo que todos los procedimientos administrativos deban ser sancionatorios, o que al imponer sanción sean más efectivos, sino

que estadísticamente el número de sanciones es mucho menor que el número de procedimientos.

Si hacemos un rápido ejercicio de calificación cuantitativa, encontraremos que, en efecto, el IFAI queda a deber en esta materia, pero tratemos de entender por qué.

El Instituto puede iniciar procedimientos administrativos por varias vías, la verificación de oficio y la denuncia son dos grandes de ellas, en ese sentido es lógica la conclusión de que han existido pocas denuncias y asumimos que proporcionalmente pocas visitas de verificación.

A qué se puede deber esto, las hipótesis pueden ser muchas, pero a mi percepción son dos; los operadores institucionales de la Ley, es decir el propio IFAI no ha administrado bien su función jurisdiccional, asumo que ha sido por sus grandes cambios administrativos, razón ésta que espero en esta nueva integración sea resuelta.

La segunda gran razón es que los operadores sociales de la Ley, es decir, nosotros los especialistas y la población en general, nos hermosa quedado cortos en el cumplimiento de la Ley, al existir pocas denuncias, considero que no es porque existe un alto nivel de cumplimiento, sino un alto nivel de desconocimiento y tal vez de confianza en la institución.

De esta suerte, somos corresponsables de esta problemática, por lo tanto podemos ser participantes de su solución, propagando la información y la cultura del respeto y la protección de los datos personales e impulsando la cultura del respeto a la misma, exigiendo su cumplimiento y en su caso, presentando las denuncias que serán un insumo primordial para que el IFAI cumpla su función.

Fuentes:

Estudio de opinión: “Mexicanos reprobados en transparencia”, consultado el 1 de octubre de 2014 en: http://www.parametria.com.mx/carta_parametrica.php?cp=4672

Estudio de opinión: “Estudio de protección de datos personales entre empresas y usuarios”, consultado el 1 de octubre en: https://www.amipci.org.mx/estudios/proteccion_de_datos_personales/2012ProteccionDeDatosPersonalesentreUsuariosEmpresasvE-1.pdf

Resoluciones del IFAI: Consultado el 1 de octubre en www.ifai.org.mx

INTEROPERABILIDAD, ACCESIBILIDAD E INCLUSIÓN DIGITAL – REALIDAD PERUANA

INTRODUCCIÓN

EDDA KAREN CÉSPEDES BABILÓN[ii]

Más allá del concepto de Interoperabilidad que la IIE y la Comunidad Europea definen como el intercambio de información de dos o más sistemas, se requiere igualmente mencionar que hacen falta importantes desarrollos en los Procesos Informáticos, la Administración Electrónica, y la Normatividad Jurídica.

Sin embargo la eficacia de esta interactividad recae en las Políticas gubernamentales cuyos procesos deberán facilitar además del intercambio de la información de manera segura, organizada y legitima, el desarrollo de un Gobierno Electrónico que verdaderamente conlleve a la Accesibilidad, la Inclusión Digital y la participación democrática de toda la ciudadanía, en una activa y dinámica gobernanza tecnológica.

En este articulo se pretende enfocar las Políticas de Gobierno Electrónico Peruano, las acciones que se viene desarrollando y los caminos que aún faltan por recorrer para dinamizar el trabajo del equipo multidisciplinario que requiere de la importante participación del Estado como líder político comprometido en la ejecución y desarrollo de la Interoperabilidad, la Accesibilidad, Interconectividad y la Inclusión Digital; acciones que requieren del responsable compromiso del Estado en sus diferentes poderes: Poder Ejecutivo, Legislativo, y Judicial, incluyendo además, los Organismos Autónomos y Gobiernos Locales.

INTEROPERABILIDAD, ACCESIBILIDAD E INCLUSIÓN DIGITAL – REALIDAD PERUANA

Sobre las materias a tratar, observamos tres diferentes conceptos cuya importante relación, trataremos de resaltar en el desarrollo de este tema.

1. INTEROPERABILIDAD

La Interoperabilidad no solo es la capacidad de dos o más sistemas informáticos para intercambiar datos entre si, como indica la IEEE[ii], sino que como bien lo amplía la Comunidad Europea, y el Marco Iberoamericano de Interoperabilidad[ii], aprobado por la XII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado[ii]; se trata en general, sobre la capacidad de diferentes organizaciones o instituciones para interactuar de forma organizada y coordinada, intercambiando información y datos, mediante los sistemas de las Tecnologías de Información y las Comunicaciones – TIC's, con el fin de alcanzar objetivos comunes y mutuamente beneficiosos. En consecuencia, al tratarse de las Instituciones Públicas, nos referimos a "Interoperabilidad" como la capacidad administrativa, técnica y política, que permite utilizar las TIC's, relevantes en el marco de un Gobierno Electrónico. En este sentido, podemos resumir que la interoperabilidad es una herramienta, que facilita la interacción organizacional en una mutua colaboración.

Asimismo, entendemos que la interoperabilidad no es un tema nuevo en nuestro ámbito, pero este concepto, ha ido enriqueciéndose y tomando

relevancia, de manera tal, que se hace imprescindible su desarrollo e implementación. De la misma forma, se hace necesario el intercambio de experiencias y conocimientos entre los países Iberoamericanos en beneficio mutuo de nuestro crecimiento tecnológico. En este sentido, el Centro Latinoamericano de Administración para el Desarrollo – CLAD viene actuando al respecto y buscando mecanismos de congruencia en los conocimientos, así como una guía para la toma de decisiones en el ámbito de la interoperabilidad.

Sin embargo, una de las principales barreras que tenemos dentro de nuestros propios Estados, son los sistemas jurídicos y las normas apropiadas que regulen nuestra actuación. Por tal motivo, la colaboración y participación de los profesionales e investigadores del Derecho en Tecnologías de la Información, se hace imprescindible proponiendo, proyectando y elaborando normas que permitan un Estado más desarrollado y moderno.

Por otro lado, y como bien sostiene el Centro Latinoamericano de Administración para el Desarrollo - CLAD[ii], la interoperabilidad requiere de estándares abiertos y software libre, con el fin de garantizar la seguridad y la sostenibilidad de un Gobierno Electrónico, y con ello, velar por los derechos y libertad de los ciudadanos, al poder elegir las tecnologías que interactuarán con las Instituciones Públicas.

Cabe resaltar, que es necesario que entre los Gobiernos y actores involucrados existan acuerdos y objetivos comunes, así como los procedimientos y formas de alcanzarlos; refieréndonos como tal, a la Gobernanza de la Interoperabilidad, que es la colaboración entre los Gobiernos Electrónicos, y conlleva a mutuos y eficaces diálogos entre los interventores del Estado.

Además de ello, la Gobernanza de la Interoperabilidad, requiere necesariamente de Normas Legales, así como de estrategias y decisiones políticas que velen por un desarrollo social sostenible. Por tal motivo es necesario distinguir tres niveles importantes de Interoperabilidad, que solo serán posibles de alcanzar mediante un trabajo en equipo multidisciplinario y de diferentes niveles jerárquicos:

1. Nivel Organizativo: Asegura la coordinación y el alineamiento de procedimientos administrativos, señalando el derrotero para una comunicación y colaboración viable entre las Entidades del Gobierno Electrónico; orientando asimismo al usuario con respecto a los servicios seguros, disponibles, accesibles e identificables para los ciudadanos.

2. Nivel Semántico: Garantiza que el significado de la información y los datos intercambiados sea comprendida con precisión por todas y cada una de las aplicaciones que intervengan, combinando y procesando la información de manera adecuada.

3. Nivel Técnico: Garantiza la preparación y viabilidad de todos los aspectos técnicos (software, hardware, telecomunicaciones), necesarios para la correcta y segura interconexión de los sistemas informáticos, transferencia de información y servicios, interfaces abiertas, integración de datos y middleware, accesibilidad o servicios de seguridad, para que trabajen en mutua colaboración.

En el Perú existen actualmente leyes y normas que amparan, protegen y ordenan la Modernización del Estado Peruano. Sin embargo la Normatividad

Jurídica muchas veces no es suficiente, si además no existe la identificación con las decisiones y estrategias políticas del Gobierno Central; tema vital que incluyen acciones a corto y mediano plazo en un desarrollo sostenible.

Al respecto, y en forma genérica, mencionaremos que desde la década de los noventa se da inicio del Internet en el Perú, sin embargo, el Estado Peruano recién logra desarrollar las políticas públicas en Gobierno Electrónico y Sociedad de la Información a partir del año 2001; estableciendo lineamientos generales para masificar el acceso a Internet en el Perú, y dando lugar al uso de las TIC's como medio para mejorar la gestión del Estado. Posteriormente viene todo un proceso de Modernización, Reforma y Gestión del Estado, tal es así, que en el año 2007 y de acuerdo al Decreto Supremo Nro.063-2007-PCM[ii], se estableció a la Presidencia del Consejo de Ministros como el Ente Rector del Sistema Nacional de Informática mediante la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI, facultándola a emitir las directivas o lineamientos correspondientes. Asimismo, en el año 2003, se crea la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información – CODESI, con el objetivo de elaborar un Plan de Desarrollo de la Sociedad de la Información cuyo proceso de trabajo se llevo a cabo mediante modificaciones y reformas que culminaron en la formulación y aprobación de la Agenda Digital Peruana 2.0.

- **LA AGENDA DIGITAL PERUANA 2.0**[ii]: Mediante Decreto Supremo Nro. 066-2011-PCM[ii] (que modifica el D.S. 031-2006-PCM), se aprobó el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0, la cual plantea como visión <llegar a ser una

Sociedad de la Información y Conocimiento, activa y productiva. Una sociedad integrada, democrática, abierta, inclusiva y que brinde igualdad de oportunidades a todos>. Asimismo, considera cinco factores de éxito:

1. El Liderazgo Político.
2. Una intervención articulada e insertada en la planificación estratégica y operativa de los tres niveles de gobierno.
3. Recursos que aporten sostenibilidad a las propuestas.
4. Institucionalización.
5. El compromiso y aprobación de las organizaciones públicas, privadas, la sociedad civil y la academia.

Esta Agenda constituye una importante contribución de políticas para el cumplimiento de los objetivos de Desarrollo del Milenio para el Perú; pues establece los lineamientos, estrategias y acciones que se deben seguir para posibilitar el acceso de todas las personas a las ventajas que se derivan de las TIC's; constituyéndolas como un instrumento de desarrollo más equitativo y sostenible, importantes en el crecimiento económico y el marco del proceso de implementación y promoción de la Sociedad de la Información en el Perú.

Cada uno de los ocho importantes objetivos sobre los cuales se sustenta la Agenda Digital Peruana 2.0 al 2015, tienen diferentes estrategias que se interrelacionan entre sí, y que promueven el desarrollo de actividades de toda la administración pública para ofrecer servicios de calidad orientados a la población. Su importante elaboración, ha sido producto

de la congruencia y trabajo en equipo del sector público, sector privado, la academia, y la sociedad civil. Pero esta multidisciplinaria labor, debe ejecutarse a corto plazo, por lo que se requiere del compromiso y puesta en marcha, a nivel Estado, para alcanzar con objetividad la Modernización y Descentralización[ii] en un esquema real de beneficios al ciudadano y la Inclusión Digital, a la que el Gobierno debe dar mayor prioridad. En este sentido se necesita que los Poderes del Estado y los Gobiernos Regionales y Locales, incluyan en sus Planes Operativos las políticas y lineamientos de la Agenda Digital 2.0, participando activamente, posicionándose en la labor de promoción, capacitación, proyectos, desarrollos e implementación, así como propuestas, mejoras y normas que amparen la realización de un gobierno más democrático y tranparente, priorizando y adecuando proyectos para las zonas más alejadas de la capital; de forma tal, que nada ni nadie nos aleje del bienestar del ciudadano como eje central, no solo para tener acceso a la Información, sino además para tomar decisiones; utilizando las TIC's como una herramienta útil que conlleve a mayores y mejores conocimientos, sistemas de educación y desarrollo sostenible. Temas tratados, y en algunos casos programas experimentados, pero que aún no logran un significado consistente en el tiempo.

Es importante resaltar que la Agenda Digital 2.0 se desarrollo en el marco de un proceso normativo, previo a las políticas en el Perú. En algunos casos, conforme nuestros procesos económicos y sociales, y en otros de manera equitativa y a largo plazo. Normas posibles de clasificar en:

- Normas de e-Government.
- Normas de Comercio Electrónico.
- Normas para el Control y Protección en la Red.
- Normas de Defensa de Derechos Fundamentales.
- Normas sobre la Sociedad de la Información y Gobierno Electrónico[ii].

Durante los últimos años el Gobierno Electrónico en el Perú ha incrementado su desarrollo a través de diferentes proyectos y acciones que han ido consolidándose en la institucionalización, organización y ejecución de diferentes programas, dirigidos y supervisados por la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI[ii], de la Presidencia del Consejo de Ministros. Como hemos observado, uno de los significativos avances ha sido la dirección e impulso de la Agenda Digital Peruana y la creación de la Comisión Multisectorial[ii] para su seguimiento y evaluación.

Otro significativo avance es la Plataforma de Interoperabilidad del Estado Peruano –PIDE, basado en la Arquitectura SOA[ii], cuyo proyecto piloto y actualmente en funcionamiento, es la Constitución de Empresas en Línea, donde intervienen cinco entidades públicas. El Proyecto se ejecuto entre los años 2007 y 2011 y ha sido todo un éxito.

- **PLATAFORMA DE INTEROPERABILIDAD DEL ESTADO PERUANO – PIDE:** Desde el 2005, se plantea y diseña el Proyecto de Gobierno Electrónico, año desde el cual se viene desarrollando y madurando el proceso de interoperabilidad en el Perú. Mediante Decreto Supremo Nro. 083-2011-PCM se aprueba la creación de la Plataforma de Interoperabilidad

del Estado – PIDE, el cual se ha convertido en el Proyecto de mayor envergadura. La Plataforma ha sido desarrollada utilizando la Arquitectura Orientada a Servicios – SOA, que haciendo uso de estándares como XML y servicios web, permite tener un conmutador central para la implementación de servicios públicos en línea en forma ordenada y planificada, por medios electrónicos seguros, y el intercambio electrónico de datos entre las Entidades Públicas, a través de Internet, telefonía móvil y otros medios electrónicos disponibles. Con esta solución tecnológica, el Perú, se afianza en el Nivel de Procesos Integrados.

Como hemos mencionado la Plataforma de Interoperabilidad – PIDE, se inicio con la Constitución de Empresas en Línea en 72 horas, a través de un trabajo participativo y en conjunto de diferentes Instituciones Públicas: El Colegio de Notarios de Lima – CNL, la Superintendencia Nacional de Registros Públicos – SUNARP, el Registro Nacional de Identificación y Estado Civil – RENIEC, la Superintendencia Nacional de Administración Tributaria – SUNAT y la Presidencia del Consejo de Ministros - PCM, entidades que interconectan sus Sistemas de Información a fin de brindar el servicio de formalización empresarial en el término de 72 horas. A pesar de que estos dos últimos años el servicio se amplió a: Cusco, Arequipa, Puno, Madre de Dios, Tumbes, Piura y La libertad, constituyéndose más de 24,000 empresas en todo el país, aun existen muchas regiones que no cuentan con esta facilidad, pero se programa ampliar su cobertura y asimismo reducir el número de horas

del proceso, en vista de que la formalización de las empresas, como las micro y pequeñas empresas, generan más puestos de trabajo.

Paralelamente, en el tema de interoperabilidad, se viene instalando un "Software del Sistema de Licencia Municipal En Línea", para las Municipalidades del Perú, que lo requieran; la articulación en la mesa de trabajo de la Superintendencia Nacional de Aseguramiento en Salud – SUNASA, para el "Registro de Afiliados"; e implementando un "Software de Visitas a las Entidades Públicas del Estado", en el marco de las políticas de Transparencia.

Asimismo se ha implementado el servicio de mensaje de texto telefónico (SMS) en la Plataforma de Interoperabilidad, ofreciendo el servicio de notificación SMS en la Región Ucayali en coordinación con el Seguro Social de Salud del Perú - EsSalud, para apoyar la lucha contra el brote de la Epidemia del Dengue. En este sentido, se programa mejorar la calidad y avanzar hacia el Gobierno Móvil o m-Government, implementando mayores servicios para todos los ciudadanos, por tal motivo se ha reactivado el Grupo de Trabajo de Interoperabilidad y del Estado - GTIE[ii].

- **PORTAL DEL ESTADO PERUANO –PEP[ii]:** El Portal del Estado Peruano fue creado en el año 2001, mediante Decreto Supremo Nro. 060-2001-PCM, como un sistema interactivo de información a los ciudadanos a través de Internet, asimismo se crearon normas afines y conexas al respecto que con los años se han ido actualizando paralelamente al avance de interoperabilidad, accesibilidad e inclusión digital.

Es el Portal de mayor jerarquía dentro del Estado y el primer acceso oficial que tienen tanto peruanos como extranjeros para conocer el Perú. En el portal se encontrará información de actualidad con las noticias más resaltantes del día; eventos y campañas llevadas a cabo por las entidades públicas; servicios para los ciudadanos: Portal para Pequeñas y Medianas empresas MYPE, Portal del Sistema Integrado de Información de Comercio Exterior, Portal de Servicios al Ciudadano y Empresas, entre otros servicios. Asimismo en la parte superior se encuentran los Portales Institucionales: Presidencia de la República, Presidencia del Consejo de Ministros, Congreso de la República y Poder Judicial; el Directorio del Estado; el Portal de Transparencia y una sección de Normas Legales, entre otras cosas muy importantes como la sección especial al Turismo para que las personas interesadas en visitar el país cuenten con toda la información necesaria.

También existen otros portales que se vienen desarrollando y actualizando, pero, entre los más importantes nombraremos al Portal de Servicios al Ciudadano y Empresas y al Portal de Transparencia:

- **PORTAL DE SERVICIOS AL CIUDADANO Y EMPRESAS:** Es la Ventanilla Única del Estado y constituye un punto de acceso claro y sencillo para las necesidades de la población. Es una aplicación en Internet que permite enlazar a páginas Web, base de datos y sistemas informáticos de las Entidades Públicas para obtener información de trámites, acceder a servicios en línea y formatos. Entre los trámites más solicitados se encuentran: la revalidación de pasaporte, antecedentes penales, obtención y duplicado del

Documentos Nacional de Identidad – DNI, duplicado de brevete, Registro Único de Contribuyentes – RUC, solicitud mediante la Ley de Acceso a la Información, entre otros. Los servicios en línea más demandados son: consulta y rectificación de estado civil, modificación de datos RUC, cuentas de ahorro Multired Virtual, etc. Y entre los formatos más solicitados: la expedición y revalidación de pasaporte, carné de extranjería, salvoconducto fronterizo, solicitud por Ley de Acceso a la Información Pública etc.[ii]

- PORTAL DE TRANSPARENCIA ESTÁNDAR: Con el objeto de estandarizar, integrar, promover la ética y dar mayor transparencia a la gestión pública, con Decreto Supremo Nro. 063-2010-PCM[ii] se aprueba la "Implementación del Portal de Transparencia Estándar en las Entidades de la Administración Pública", que ordena establecer los lineamientos para uniformizar el contenido de la información de los Portales de Transparencia[ii]. La información que se publica está referida a datos generales de las entidades públicas, información de personal, planeamiento y organización, información financiera y presupuestaria, actividades oficiales, participación ciudadana, información sobre proyectos de inversión, contrataciones de bienes y servicios e información adicional[ii].

Es un Portal de información único, integral y estandarizado, para mejorar y dar mayor transparencia a la gestión pública. Cuenta con iconos ilustrativos y amigables, ayuda en los textos técnicos y

semaforización en los estados de los iconos, lo que permite distinguir la sección que estamos utilizando.

2. ACCESIBILIDAD

Si queremos hacer un Estado más justo y transparente, debemos partir de la "Igualdad", entre otros Derechos Fundamentales. La "Igualdad" debe aplicarse en todo campo, situación y Sociedad que se jacte de crecimiento tecnológico y democrático. Es por eso que todo ciudadano, sin discrimación alguna, debe tener las facilidades para: poder utilizar un objeto, visitar cualquier lugar o sitio, y en general, tener acceso a todas las facilidades y servicios que brinda el Estado; sin que las capacidades físicas o limitaciones funcionales, sean un obstáculo. Es decir, que el acceso a la tecnología tiene que ser por igual y en las mismas condiciones, refiriéndonos con ello, a la accesibilidad Web; cuyos contenidos deben ser diseñados pensando en el acceso de todos los usuarios; que incluye, a las personas con discapacidad. Como ejemplo podemos decir, que si ponemos un video en la Web con subtítulos, será fácil de entender para las personas con dificultades auditivas; o, si ponemos en la Web una imagen con lectura de texto, como sustituto o alternativo, permitirá a los usuarios con incapacidad visual, utilizar lectores de pantalla, para acceder al contenido.

La iniciativa de facilitar el acceso a las personas con discapacidad, parte de la actividad desarrollada por el W3C[ii], que no solo señala las pautas para desarrollar una Web más accesible, sino además, mejora las herramientas de evaluación y reparación, abriendo nuevos campos de investigación en este tema.

Ahora bien, nos estamos refiriendo a un acceso universal a la Web, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de los usuarios. Es decir, una página Web accesible, debe serlo, para todos los usuarios, como ya hemos indicado, y esto incluye a las personas con discapacidad y a las personas que por diferentes circunstancias externas, (como letras pequeñas, atención visual o auditiva no disponible, ruidos externos etc.) se sientan imposibilitados de acceder a la Web.

- **ACCESIBILIDAD WEB – GOBIERNO PERUANO:** En el Perú, con Resolución Ministerial Nro. 126-2009-PCM, se aprueban los Lineamientos para la Accesibilidad a Páginas Web y Aplicaciones para Telefonía Móvil; estableciendo las técnicas y pautas, que ayudarán a las Entidades Públicas en la elaboración de contenidos accesibles; mejorando sus páginas web y sentando las bases para el desarrollo de las aplicaciones a utilizar en equipos móviles. Todo ello, dentro del marco de la Sociedad de la Información, la Inclusión Social y la accesibilidad a los discapacitados visuales y otros.

  La norma recoge los objetivos que se encuentran planificados dentro del Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana. Asimismo, se resalta el uso de Internet y la Telefonía Móvil como importantes herramientas tecnológicas para ampliar la cobertura de los servicios públicos del Estado, mediante aplicaciones informáticas y software[ii], basados en estándares mundiales que permitan su funcionamiento y la implementación de los servicios en

línea. Cabe resaltar que los Lineamientos de Accesibilidad indican que no son las únicas técnicas que un desarrollador Web, puede seguir para crear contenidos conforme a las pautas; pero si es clara la norma al ordenar la implementación de estos Lineamientos para la Accesibilidad a las páginas Web de todas las Entidades Públicas; con la supervisión, orientación y asesoría respectiva de la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI de la Presidencia del Consejo de Ministros –PCM.

En general se trata de catorce pautas que proporcionan soluciones de diseño, ofreciendo flexibilidad bajo diferentes situaciones y proporcionando métodos que permitan elaborar páginas útiles e inteligibles, a su vez, se muestran algunos ejemplos de situaciones comunes sobre problemas de acceso a la información. Cabe resaltar, que las pautas contienen puntos importantes de verificación que ayudan a detectar probables errores. Cada punto de verificación tiene asignado, uno de los tres niveles de prioridad establecidos para las pautas[ii].

La accesibilidad, tiene por objeto la inclusión digital.

3. INCLUSION DIGITAL:

En las últimas décadas, uno de los principales objetivos de los Estados, a nivel mundial, es la Inclusión Social. La Inclusión Social implica que todos los ciudadanos, sin excepción alguna, gocen, por derecho, de todos los servicios que brinda el Estado; en un proceso dinámico que les permita interactuar, desarrollarse y mejorar su calidad de vida. En este sentido, para lograr,

verdaderamente una Inclusión Social, especialmente cuando se trata de personas con discapacidad física o intelectual; se requiere de un arduo trabajo y múltiples apoyos, además de un cambio esencial en la mentalidad social[ii].

Al referirnos a la Inclusión Digital, estamos mencionando uno de los mayores objetivos de la Inclusión Social, que además de lo mencionado en el párrafo anterior, permitirá el acceso de todos los ciudadanos a las Tecnologías de la Información y las Comunicaciones – TIC's utilizando y desarrollando sus capacidades. Este contexto, abarca no solo el acceso a Internet, sino además, el conocimiento y uso beneficioso de las TIC's como herramientas a través de las cuales se obtengan mejores niveles educativos, sociales, participativos y productivos.

- **INCLUSION DIGITAL EN EL PERÚ: YACHAYWASI DIGITAL:** Conforme el cuarto objetivo estratégico de la Política Nacional de Gobierno Electrónico 2013-2017, que señala: "*Fomentar la inclusión digital de todos los ciudadanos, especialmente a los sectores vulnerables, a través de la generación de capacidades y promoción de la innovación tecnológica, respetando la diversidad cultural y el medio ambiente";* es que el Estado viene acrecentando el Proyecto de Inclusión Digital a través de la creación de espacios, donde se capacita a los ciudadanos en programas de Alfabetización Digital.

  A este tipo de espacios se le ha denominado:"Yachaywasi Digital". Yachaywasi, es una palabra en quechua que significa "Casa del Saber" y era el lugar donde los adolescentes varones, de la Nobleza Incaica se instruían en los conocimientos de Administración y Gobierno.

El primer nivel de Alfabetización Digital consiste en dar a conocer a los ciudadanos el uso de Internet y la Tecnologías de la Información – TIC's; desarrollar habilidades para su aprendizaje, socialización e interacción en el mundo virtual y mejorar sus capacidades productivas a través de las tecnologías, orientándolos a promover el aprendizaje en relación al desarrollo de la Comunidad y sus proyectos aplicables por parte de los ciudadanos. El segundo nivel consiste en capacitar a los funcionarios y servidores públicos de las entidades públicas, principalmente en los Gobiernos Regionales, acrecentando su desarrollo en las tecnologías y motivándolos como promotores e impulsadores del cambio a la Sociedad de la Información.

Además de ello, el Yachaywasi Digital, capacita a los jóvenes, mujeres y productores en temas de Marketing Digital, Comercio Electrónico, Constitución de Empresas en línea y otros necesarios para que la Comunidad se desarrolle y progrese. Estas capacitaciones se realizan gratuitamente y de manera virtual, utilizando la plataforma "e-learning[ii]"; lo cual permite llevar a cabo cursos virtuales, con asesoramiento y seguimiento en línea para todos los miembros de la Comunidad.

Yachaywasi Digital, se implemento en el año 2013 en la Zona del VRAEM[ii], posteriormente se instalaron otros dos en Huamanga y Huaraz; y próximamente se abrirán otros en Cuzco, Piura y Lima, continuando de esta manera con el despliegue nacional.

El crecimiento y desarrollo de mayores Proyectos de Inclusión Digital también se fundamenta en la Ley 29904 – Ley de Promoción de la Banda

Ancha y Construcción de la Red dorsal Nacional de Fibra Óptica, publicada el 20 de Julio 2012[ii], cuyo objetivo es impulsar el desarrollo, utilización y masificación del acceso a Internet de forma permanente y a alta velocidad, además, y de acuerdo a los dispuesto en la Ley, la Banda Ancha contribuye al efectivo ejercicio de los derechos fundamentales de la persona y al desarrollo económico del país; recogiendo en sus artículos 23 y 24 la importancia de la alfabetización digital y los espacios de acceso público con conexiones de banda ancha para que la población acceda a contenidos y aplicaciones de Gobierno Electrónico, además de considerarlos, como espacios de formación de capacidades para su aprovechamiento. Es después de más de diez meses que se promulga su Reglamento con el Decreto Supremo 014-2013-MTC[ii], que marca los lineamientos y políticas de su aplicación. Este proyecto del Estado Peruano busca además promover la libre competencia y abaratar costos en telecomunicaciones, haciendo más accesible su uso en todos los estratos sociales.

4. CAMBIANDO PARADIGMAS EN POS DE LA JUSTICIA Y EL DERECHO A TRAVÉS DE LAS TECNOLOGÍAS

Si analizamos los tres puntos atribuidos a este tema, como son: la Interoperabilidad, la Accesibilidad y la Inclusión social, encontramos que su estudio y aplicación conllevan a entrelazarlos, manteniendo una congruencia y relación entre ellos, necesaria y conveniente en el marco de los objetivos de un Gobierno Electrónico, cuyo eje es el ciudadano, como ya hemos mencionado; pero principalmente, respetando el concepto de desarrollo como libertad que contempla la Declaración Universal de los Derechos

Humanos, y los derechos fundamentales exigidos en Nuestra Carta Magna, en bien de una verdadera participación ciudadana, con las facilidades que las Tecnologías, actualmente nos ofrecen.

Esta revolución tecnológica nos permite, progresivamente, ampliar nuestros conceptos, rompiendo barreras y cambiando paradigmas, con el fin de llegar a nuevas metas, no solo para desarrollar un Gobierno Electrónico, sino además de ello, para hacer sostenible y efectiva la participación ciudadana a través de acciones inmediatas por parte del Estado que conlleven al GOBIERNO DE LA INFORMACIÓN. Caso contrario, no podríamos referirnos a Igualdad Social, ni Libertad y Justicia para todos, sin contar con facilidades que nos permitan ejercer nuestros derechos y al mismo tiempo, hacer valer nuestras opiniones, en temas que contribuyan al verdadero crecimiento de un Estado democrático, valedero y participativo.

No existe una definición exacta de "Gobierno de la Información" pero podemos conceptuarlo como el conjunto de procesos y tecnología que permiten a una organización optimizar, proteger y aprovechar mejor sus datos[ii]. Este concepto ha ido evolucionando por la visión del progreso tecnológico a nivel mundial, que ha motivado el quehacer de muchos Estados Iberoamericanos en la actualización de estrategias y cambios en sus políticas de Estado, con el fin de conseguir el desarrollo de la Sociedad de la Información. En este sentido, el Centro Nacional de Planeamiento Estratégico – CEPLAN, publicó, el año pasado el "Plan Bicentenario, el Perú hacia el 2021", (aprobado por el Acuerdo Nacional, en Marzo del 2011), documento que mediante Ejes Estratégicos, marca los objetivos, lineamientos, prioridades y programas, que deben orientar las decisiones y acciones del Estado, a bien de

alcanzar las metas de desarrollo al 2021[ii]. Sin embargo, con la finalidad que se afiance el crecimiento con inclusión social en democracia; la igualdad de derechos, oportunidades, y metas sociales alineadas con los objetivos del milenio; se alcance la concertación económica y social en el ámbito nacional, regional y local; y se logre el reencuentro histórico con el Perú rural; en diciembre 2013, CEPLAN presentó ante la Presidencia del Consejo de Ministros – PCM, para su aprobación, la última versión actualizada del Plan Estratégico de Desarrollo Nacional denominado "Plan Bicentenario"[ii], proceso que se llevo a cabo con la participación de diferentes instituciones, gremios, colegios profesionales, organismos y ciudadanía en general, entre otros, conforme lo indica el Decreto Supremo Nro.051-2012-PCM[ii]. Asimismo, y siguiendo la misma estrategia de Modernización de la Gestión Pública[ii], sus planes y políticas[ii]; así como la actualización normativa; es que se aprueba con Decreto Supremo Nro. 081-2013-PCM[ii], la Nueva Política Nacional de Gobierno Electrónico, considerando importante el uso de las tecnologías de la información en el marco del desarrollo del país con el incremento de la competitividad; el acercamiento del Estado a los ciudadanos de forma inclusiva; la promoción de la participación ciudadana; la transparencia y el acceso a la información pública; así como la mejora de la gestión pública y la seguridad de la información.

Según lo manifestado, ya no se trata sólo de una conexión con algún Ministerio o Institución Pública, para obtener una información, realizar gestiones en línea, o dejar un mensaje esperando una respuesta, que nunca llega. Se trata, de incluir, además del óptimo acceso a los servicios de información y gestiones, que ofrecen las Entidades Públicas; se incluyan también, servicios de consultas

en línea, que además le permita al ciudadano emitir aportes de mejora u opinión al respecto, permitiendo con ello la posibilidad de interconectarse e interactuar a diferente nivel, con las autoridades responsables de las Instituciones Públicas, quienes comprometidos en la solución, respecto de la consulta u opinión, realizarán un seguimiento del caso, hasta su culminación, según sea necesario. Demás, esta señalar que la transparencia y respeto al ciudadano, es vital para generar confianza y libre opinión. Asimismo cabe resaltar, la importancia de las políticas de Seguridad Informática[ii] las cuales, desempeñan un rol preponderante en el uso de las Tecnologías de la Información. Pero lo principal es el cambio de actitud y la sensibilización a las Entidades de Gobierno para brindar al ciudadano una preferente atención, cordialidad y sobretodo absolver sus consultas, tomando en cuenta sus opiniones. En esto radica principalmente el cambio de paradigma, que la tecnología nos facilita, pero que a la vez nos exige el reto de hacer que el ciudadano se sienta el eje de la sociedad.

En esta línea de información y participación ciudadana, actualmente en el Portal del Estado Peruano, podemos encontrar una sección denominada "Directorio de las Redes Sociales"[ii], que describe a las Entidades Públicas que cuentan con Redes Sociales como Facebook, Twitter, YouTube, o G+, a las cuales se puede acceder fácilmente. Al respecto hemos apreciado que, si bien, el acceso es abierto a toda la ciudadanía, y las Redes pueden ser visitadas por muchas personas; aún nos parecen pocos los ciudadanos que dejan algún comentario o participan activamente de esta facilidad; por eso, creemos necesario profundizar más el trabajo de sensibilización digital y conseguir la

confianza y participación de la ciudadanía velando por su libertad de expresión entre otras prioridades.

Por otro lado, y como ya hemos enfocado en algunos otros artículos y exposiciones, la importancia de las estrategias públicas, juega un rol preponderante en la prioridad del Presupuesto del Estado para inversiones de tecnología, ya que muchas veces resultan ser insuficientes; por un lado, por la falta de sensibilización y compromiso de ciertos mandos y autoridades públicas, y por otro lado por la deficiencia de infraestructura en algunas zonas del país; principalmente las zonas rurales, cuyo desarrollo se imposibilita por la falta de financiamiento; es por eso que la confianza de la Inversión Privada; especialmente los Operadores de las Redes de Telecomunicaciones, es de suma importancia, para participar y comprometerse con los principios y políticas de la Ley 29904, Ley de Promoción de Banda Ancha y construcción de la Red Dorsal de Fibra Óptica y su Reglamento. En este sentido, estamos avanzando; y es por eso que el 17 de Junio 2014, se firmó el primer contrato de Concesión del Proyecto Red Dorsal Nacional de Fibra Óptica: Cobertura Universal Norte, Cobertura Universal Sur y Cobertura Universal Centro" impulsado por el Ministerio de Transportes y Comunicaciones – MTC, a través del Fondo de Inversión en Telecomunicaciones[ii]; el Proyecto Integral de Telecomunicaciones comprende dos componentes: Transporte y Acceso; habiendo sido adjudicado el primer componente a la empresa Azteca Comunicaciones Perú S.A.C., del grupo Salinas de México; el segundo componente de Acceso de Telecomunicaciones, se someterá a Licitación en los próximos meses junto con los proyectos regionales complementarios; marcando así, un hito importante en el Estado Peruano en los proyectos de

Inclusión Social, ya que unirá 21 capitales de la región y 180 capitales de provincia a través de unos 13,400 kilómetros de fibra óptica, lo cual permitirá hacer más viable y fructífera la tecnología para todos los pueblos del Perú.

Como hemos visto, el derecho y las leyes, han ido avanzando en convergencia con muchas disciplinas estos últimos años, sin embargo, con respecto a la tecnología aún hay dificultades en algunos aspectos, situaciones y hechos que jurídicamente no han sido cubiertos en nuestro país, debido al vertiginoso avance tecnológico. Por tal motivo, el quehacer del profesional del derecho, ha debido dar un vuelco enorme, de un tiempo a esta parte, poniéndose al día, actualizándose y sumándose a esta revolución tecnológica, que conlleva a una constante investigación y congruencia de ideas, propuestas y mecanismos jurídicos, que contemplen normas y reglas en bien del ciudadano en general. Así también muchos organismos públicos y privados están convocando a profesionales del derecho conocedores y especialistas en TIC's, a bien de aportar temas de seguridad jurídica en todos los campos y disciplinas.

Pero, aún hay mucho por hacer y a pesar de que la Encuesta de Gobierno Electrónico 2014 del Departamento de Asuntos Económicos y Sociales de las Naciones Unidas[ii] indica que el Perú ha subido diez lugares en el Ranking Mundial de Gobierno Electrónico, aun tenemos una brecha digital que deberemos reducir, y esperamos hacerlo pronto, considerando que la Presidencia del Consejo de Ministros – PCM, estimo una inversión de USDL4000 millones para la tecnología del 2014[ii], lo que representa un incremento de 8.1% en relación al año anterior, es por eso la necesidad de redoblar esfuerzos, identificar acciones y ejecutarlas con inmediatez en aras

de mejorar la calidad, accesibilidad e interoperabilidad, abanderadas por el respeto a los derechos fundamentales, justicia social e Inclusión Digital.

FUENTES Y RESEÑAS:

[ii] http://www.ieee.org/education_careers/education/standards/standards_glossary.html Portal del Instituto de Ingenieros Eléctricos y Electrónicos - Glosario

[ii] http://www.conavi.go.cr/wps/wcm/connect/d95de7a7-d294-447f-adcc-017d7ddce9ef/5-1Bases+para+una+estrategia+iberoamericana+de+interoperabilidad.pdf?MOD=AJPERES&CACHEID=d95de7a7-d294-447f-adcc-017d7ddce9ef Bases para una Estrategia Iberoamericana de Interoperabilidad – XX Cumbre Iberoamericana – Argentina 2010

[ii] http://old.clad.org/documentos/declaraciones/consenso-de-buenos-aires Centro Latinoamericano de Administración para el Desarrollo. XII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado. Consenso de Buenos Aires 2010

[ii] http://www.clad.org Portal: Centro Latinoamericano de Administración para el Desarrollo

[ii] http://www2.pcm.gob.pe/Transparencia/Doc_Gestion/DS-063-2007-PCM.pdf Decreto Supremo que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros. D.S.-063-2007-PCM publicado el 14 de julio 2007 en el Diario Oficial El Peruano.

[ii] http://www.codesi.gob.pe La Agenda Digital 2.0

[ii] http://www.codesi.gob.pe/docs/AgendaDigital20_28julio_2011.pdf D.S.066-2011-PCM Aprueban el Plan de desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0 – Dado en la Casa de Gobierno de Lima a los veintiséis días del mes de julio del año dos mil once.

[ii] http://www.pcm.gob.pe/InformacionGral/sgp/2009/Leyes_de_Modernizaci%C3%B3n.pdf Referentes Básicos para la mejora de la Administración Pública – Parte II - Leyes de Modernización del Estado Peruano

[ii] Presidencia del Consejo de Ministros – PCM, Oficina Nacional de Gobierno Electrónico e Informática – ONGEI –Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital 2.0 –Página 29 - Segunda reimpresión: Febrero 2013. 1. Normas de e-Government: a) Ley 27269, Ley de Firmas y Certificados Digitales. Reglamento de la Ley de Firmas y Certificados Digitales aprobado mediante D.S. 052-2008-PCM, modificado mediante D.S. 070-2011-PCM. b) Notificaciones Electrónicas, regulada mediante Ley 27444 (artículo 20.4), modificada mediante D. Legislativo 1029. c) Ley 28612, Ley que norma el Uso, Adquisición y Adecuación del Software en la Administración Pública. 2. Normas que favorecen el comercio electrónico: a) Ley 27291, Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica. – Capítulos de Comercio Electrónico (explícitos) en los diversos Tratados de Libre Comercio (TLC): Perú-Canadá - Capitulo Quince de Comercio Electrónico, Perú-Corea del Sur - Capítulo Catorce de Comercio Electrónico, Perú-EFTA (Estados de la Asociación Europea de Libre Comercio) – Artículo 1.8 de Comercio Electrónico, Perú-Estados Unidos - Capítulo Quince de Comercio

Electrónico, Perú-Singapur – Capitulo Trece de Comercio Electrónico. 3. Normas para el control y protección en la red: a) Ley 27309, - Ley que incorpora los Delitos Informáticos al Código Penal. b) Ley 28493 - Ley que regula el Correo Electrónico Comercial no solicitado (spam). c) Ley 28119, modificada por la Ley 29139, Ley que Prohíbe el Acceso a Menores de Edad a Páginas Web de Contenido Pornográfico y a cualquier otra Forma de Comunicación en Red de Igual Contenido, en las Cabinas Públicas de Internet, y su Reglamento aprobado mediante D.S. 025-2010-ED. d) R.M.360-2009-PCM, mediante la cual crean el Grupo de Trabajo denominado Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT) Normativa de creación del PeCERT. 4. Normas de defensa de derechos fundamentales: a) Ley 29733 – Ley de Protección de Datos Personales. b) Ley 29603, Ley que autoriza a la Oficina Nacional de Procesos Electorales (ONPE) a emitir las Normas Reglamentarias para la Implementación Gradual y Progresiva del Voto Electrónico. c) D.S.043-2003-PCM, que aprueba el TUO de la Ley 27806 – Ley de Transparencia y Acceso a la Información Pública. 5. Normas sobre la Sociedad de la Información y Gobierno Electrónico: a) R.M.274-2006-PCM, mediante la cual se aprueba la Estrategia Nacional de Gobierno Electrónico. b) R.M.081-2003-PCM, mediante la cual se crea la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información (CODESI). c) D.S.031-2006-PCM, mediante el cual se aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana". d) D.S.048-2008-PCM, mediante el cual se aprueba la reestructuración de la Comisión Multisectorial para el Seguimiento y Evaluación del "Plan de Desarrollo de la Sociedad de la Información en el Perú

– La Agenda Digital Peruana". e) R.M.346-2008-PCM, mediante la cual se aprueba el Reglamento Interno de la Comisión Multisectorial Permanente para el Seguimiento y Evaluación del "Plan de Desarrollo de la Información – La Agenda Digital Peruana".

[ii] http://www.ongei.gob.pe/normas/0/NORMA_0_DECRETO%20SUPREMO%20N%C2%BA%20067-2003-PCM.pdf D.S.067-2003-PCM – Por primera vez, en el año 2003, se refiere a la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI como la oficina responsable de dirigir y supervisar el Sistema Nacional de Informática y las políticas de Gobierno Electrónico.

[ii] http://www.codesi.gob.pe/presentacion/codesi_quienes.php Comisión para el Seguimiento del Plan de Desarrollo de la Sociedad de la Información – CODESI – ¿Quiénes Somos? Visión, Misión y Objetivos – Julio 2007

[ii] http://www.desarrolloweb.com/articulos-copyleft/articulo-definicion-soa.html SOA: Arquitectura Orientada a Servicios (Service Oriented Architecture)

[ii] Presidencia del Consejo de Ministros – Oficina Nacional de Gobierno Electrónico e Informática ONGEI "Una mirada al Gobierno Electrónico en el Perú –La oportunidad de acercar el Estado a los ciudadanos a través de las TIC - Primera Edición – Octubre 2013 – Pág.51.

[ii] http://www.peru.gob.pe Portal del Estado Peruano.

[ii] Fuente: Oficina Nacional de Gobierno Electrónico e Informática ONGEI – Presidencia del Consejo de Ministros PCM.

[ii] http://www.ongei.gob.pe/Bancos/banco_normas/archivos/Ds_063_2010_PC

M.pdf Decreto Supremo 063-2010-PCM publicado el 03 de junio 2010 en el Diario Oficial El Peruano.

[ii] http://www.peru.gob.pe/transparencia/pep_transparencia.asp Portal de Transparencia del Estado Peruano.

[ii] Presidencia del Consejo de Ministros – Oficina Nacional de Gobierno Electrónico e Informática ONGEI "Una mirada al Gobierno Electrónico en el Perú –La oportunidad de acercar el Estado a los ciudadanos a través de las TIC - Primera Edición – Octubre 2013 – Pág. 57.

[ii] www.w3c.com Organización que establece estándares sobre accesibilidad (WAI), mundialmente aceptados.

[ii] http://www.alegsa.com.ar/Dic/software.php Diccionario de Informática y Tecnología. Consulta: 17 de Julio 2014.

[ii] http://www2.pcm.gob.pe/Transparencia/Resol_ministeriales/2009/RM-126-2009.pdf Aprueban lineamientos para Accesibilidad a páginas web y Aplicaciones para telefonía móvil para instituciones públicas del Sistema Nacional de Informática R.M.126-2009-PCM. Firmado el 25 de marzo 2009 por el Sr. Yehude Simon Munaro, Presidente de Consejo de Ministros.

[ii]

http://www.inclusionperu.com/index.php?option=com_content&view=category&layout=blog&id=51&Itemid=118 Proyecto Inclusión Perú. Consulta: 18 de Julio 2014.

[ii] http://www.e-abclearning.com/queesunaplataformadeelearning Web: e-ABC. Consulta: 18 de julio 2014.

[ii] Valle del Rio Apurímac, Ene y Mantaro - Perú

[ii] http://www.fitel.gob.pe/archivos/FI500aa46173dcc.pdf Ley 29904 Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica. Publicada en el Diario Oficial El Peruano el viernes 20 de julio de 2012.

[ii] http://www.mtc.gob.pe/portal/comunicacion/politicas/normaslegales/REGLAMENTO.pdf Decreto Supremo 014-2013-MTC Reglamento de la Ley 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica. Publicada el lunes 04 de noviembre de 2013 en el Diario Oficial El Peruano.

[ii] ftp://ftp.software.ibm.com/la/documents/imc/la/co/swg_bogota/banca/entregue_informacion_confiable_y_obtenga_mejores_resultados_de_negocio_guillermo_estrada.pdf IBM Software Solutions Forum – Integración y Gobierno de la Información por Guillermo Estrada - Marzo 2011

[ii] http://www.ceplan.gob.pe/documentos/plan-estrat%C3%A9gico-desarrollo-nacional-per%C3%BA-2021 Plan Estratégico de desarrollo Nacional Perú al 2021. Centro Nacional de Planeamiento Estratégico – CEPLAN de la Presidencia del Consejo de Ministros.

[ii] http://ceplan.gob.pe/noticias/ceplan-culmina-version-actualizada-del-plan CEPLAN culmina versión actualizada del Plan Bicentenario. Consulta: 21JUL2014.

[ii] http://www.peru.gob.pe/docs/PLANES/13103/PLAN_13103_2014_DS_051-2012-PCM.pdf Decreto Supremo Nro. 051-2012-PCM “Ampliación de plazo para la presentación de la propuesta del Plan Estratégico de Desarrollo

Nacional actualizado" publicado en el Diario Oficial El Peruano el 06 de mayo 2012.

[ii] http://www.pcm.gob.pe/normaslegales/2013/DS-004-2013-PCM.pdf Decreto Supremo 004-2013-PCM Aprueba la Política Nacional de Modernización de la Gestión Púbica. Publicado en el Diario Oficial El Peruano el 09 de enero 2013.

[ii] http://sgp.pcm.gob.pe/index.php/lines-de-accion/modernizacion-gestion-publica/plan-modernizacion Web: Secretaría de Gestión Pública de la Presidencia del Consejo de Ministros. Consulta 21de julio 2014

[ii] http://www.pcm.gob.pe/normaslegales/2013/DS-081-2013-PCM.pdf D.S.081-2013-PCM Decreto Supremo mediante el cual se aprueba la Política Nacional de Gobierno Electrónico 2013-2017. Publicado el 10 de Julio 2013 en el Diario Oficial El Peruano.

[ii] http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica Wikipedia - La Enciclopedia libre. Referencia: Seguridad Informática.

[ii] http://www.peru.gob.pe/redessociales Portal del Estado Peruano – Directorio de Redes Sociales – Consulta Julio 2014.

[ii] https://www.youtube.com/user/FitelPeru Video de Firma del Contrato de Concesión de la Red Dorsal Nacional de Fibra Óptica - 17 de Junio 2014. Lima-Perú

[ii]

http://www.ongei.gob.pe/noticias/ongei_noticias_detalle.asp?pk_id_entidad=1878&pk_id_noticia=535 Web: Perú Gobierno Electrónico – Noticia del 25 de junio 2014 Consulta 23 de Julio 2014.

ii

http://www.ongei.gob.pe/noticias/ongei_noticias_detalle.asp?pk_id_entidad=1878&pk_id_noticia=534 Web: Perú Gobierno Electrónico. Noticia del 25 de junio 2014. Consulta: 24 de Julio 2014.

Correo Electrónico, herr@mienta de cambio

Introducción

Prácticamente todos los servicios ofrecidos en internet e incluso aquellos de la vida física, estén relacionados o no con el comercio, utilizan como un medio

de comunicación, para efectos legales un servicio de comunicación llamado “Correo Electrónico” o simplemente “email”.

El email se ha convertido en un arma muy poderosa para dar cumplimiento a obligaciones de comunicación y notificación, las legislaciones en general de más en más, le imponen cargas, validez y consistencia respecto de procesos legales.

Su inserción en Internet forma desde hace tiempo un vínculo indisoluble, somos totalmente dependientes, y precisamente ése es el gran riesgo que se analiza desde la óptica del Derecho, ya que existe por un lado en el carácter protegido respecto de las comunicaciones, como derecho humano, y dentro del cual se analizará si se encuentra el correo electrónico, y por otro lado, la ausencia armonizada de reglas o normatividad al respecto, por lo que cabe considerar respecto de si es necesaria la existencia de ordenamientos jurídicos, ya que dicho domicilio electrónico es normalmente propiedad de un proveedor de servicios de internet (ISP), o de una entidad corporativa respecto de la cual se prestan servicios como empleado o de otra forma, lo cual permite unas líneas de análisis para saber si la ciencia jurídica se encuentra acorde en el uso de éstos correos electrónicos en sus procesos de justicia dando un claro valor o se requiere de una normatividad al respecto.

El análisis parte de los aspectos legales que reviste su titularidad, uso, (particularmente como identificación e incluso de autenticación), derechos y obligaciones en general, profundizando en aquellos aspectos técnicos y formula conceptual que derive en la necesaria certeza jurídica para los usuarios y los riesgos inherentes y sus soluciones.

Conceptos

El Correo electrónico, es un servicio de red que dentro de Internet usa el protocolo SMTP que permite a quienes lo usan enviar y recibir mensajes de datos o simplemente correos (también denominados mensajes electrónicos o cartas electrónicas). A dichos mensajes se pueden integrar textos, imágenes, sonido, e inclusive ciertos programas de cómputo. Su facilidad de uso y gratuidad han hecho que se desplace al correo ordinario para muchos usos habituales.

Inicialmente en una demostración del MIT[ii] de 1961, se exhibió un sistema que permitía a varios usuarios ingresar a una IBM 7094 desde terminales remotas, y así guardar archivos en su sistema de almacenamiento, con lo cual, se hizo posible contar con nuevas formas para compartir información. El correo electrónico antecede a Internet, y fue crucial su uso en su origen. En 1971, se incorporó el uso de la arroba (@)[ii] como divisor entre el usuario y la computadora en la que se alojaba el mensaje, ya que dicho símbolo no se contenía en ningún nombre o apellido.

El correo electrónico requiere de un proveedor de la tecnología de comunicación, los enlaces, los respectivos dominios y el hardware necesario para alojar los llamados “buzones” que son simplemente porciones de espacio de almacenamiento en un medio físico, estos funciones pueden estar concentradas en una entidad o en pluralidad de entidades, pudiendo ser un servicio gratuito o de pago. El registro permite tener una dirección de correo personal única al que se puede acceder mediante un nombre de usuario y una Contraseña.[ii]

Aspectos legales

Inicialmente tenemos considerado en la Declaración Universal de Derechos Humanos el Derecho al honor, a la vida privada y a la información, que indica en su Artículo 12 “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia…”. Y en el Artículo 19 “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”. Ambas provisiones consideran desde mi óptica y en la integral interpretación que se debe realizar que tanto a la correspondencia como a la libertad de expresión se encuentran íntimamente vinculadas, ya al referirse en el segundo a “… recibir informaciones y opiniones y el de difundirlas” no únicamente es a aquellas contenidas en medios públicos, sino cualquier medio de comunicación.

Sin ahondar más, ya que las mismas disposiciones prácticamente se replican en los principales ordenamientos legales internacionales incluyendo los regionales[ii], tenemos que el correo electrónico se encuentra vinculado a la inviolabilidad de la correspondencia y comunicaciones y también derecho a comunicar o recibir informaciones en el sentido indicado. Al respecto cabe aclarar que el email es una forma de comunicación inmersa en Internet, pero además permite que se enraíce en otros medios electrónicos, ópticos o de cualquier otra naturaleza equivalente como se induce en el comercio electrónico[ii].

En legislaciones locales tanto a nivel constitucional como de legislación secundaria[ii] se han incorporado dichos conceptos, aparece en la Constitución Española, Art. 18 ..."3. …Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

Es imposible disociar dentro del entorno virtual de las comunicaciones la plataforma (Internet y otras) del programa que realiza la comunicación propiamente dicha activa la transferencia de mensajes, por lo que cabe claramente identificar la naturaleza del derecho humano que está involucrado ahí.

En relación con las características legales que se dan en la ”suscripción” al servicio de correo electrónico, debemos mencionar que en todos los casos son normas de adhesión, contenidos fundamentalmente en los llamados “Términos y Condiciones de Uso” que de los principales analizados Google, Hotmail y Yahoo consisten en la creación de una cuenta en la que se proporciona información personal y la creación de una contraseña de acceso o ”password” siempre estático, que inicialmente permite o solo la descarga del programa de cómputo que cada operador utiliza para que quien proporciona la información tenga una dirección de correo electrónico o inicie en la utilización de una “Bandeja” o archivo en los términos ya mencionados. Al respecto el primer punto a considerar es que si estamos en presencia de un contrato o elemento jurídico que permita la menos contar con tres elementos fundamentales, la expresión del consentimiento, el objeto, y los elementos accesorios. Por lo que hace al objeto y elementos, los analizados lo señalan, sin embargo no con la precisión debida, respecto del consentimiento, efectivamente si no se oprime dentro el cuadro de aceptación no se accede al programa y servicio requerido por lo que es consistente la expresión del consentimiento.

Concluyéndose de lo anterior, que si existe la vinculación legal entre las partes, sin embargo queda inconcluso saber el tipo de contrato ya que en éste sentido son poco claros sino que omisos pero consideremos para efectos que se trata de una derecho de uso y pasando al siguiente problema toral, que corresponde evidentemente el carácter que como usuario tengo respecto de “mi correo electrónico” y de todo lo que por ahí transita. Si soy usuario y hablamos de

medios electrónicos, por lo que estamos en presencia de una licencia que nos permite usar el software y una porción de un repositorio central de datos, pero no más.

Como indicábamos, los derechos humanos contemplan la inviolabilidad de la correspondencia y el domicilio, y estamos precisamente hablando en el mundo virtual, de ambos conceptos al hacerlo del email, y sin embargo, el proveedor, licenciante y dueño de mi correo electrónico tiene conforme a los términos y condiciones de uso de hacer con él y con el contenido, lo que considere ya que he otorgado en él consentimiento tácito expresado, una licencia mundial para que utilicen el contenido y además que den si así lo considera de baja mi buzón de correo y re-asignarlo a alguien más[ii].

Lo mismo sucede en el caso de los correos electrónicos asignados para su uso dentro de las entidades a las que se le prestan servicios, sean laborales o de otra índole, dicha entidad permite el uso para fines por ambas partes acordadas, fundamentalmente para un objeto común o de negocio, y en el mismo sentido, pero sin mediar expresión de consentimiento normalmente, se indican en el caso laboral de un derecho contenido en las condiciones de trabajo, un derecho a la intromisión "lícita" al contenido del buzón de sus trabajadores, y otros derechos relacionados con el correo electrónico asignado, a mi parecer sin dar cumplimiento al derecho de inviolabilidad de las comunicaciones y domicilio. La Agencia Española de Protección de Datos se ha pronunciado adicionalmente bajo el Informe 0437/2010, indicando que en

aquellos supuestos en que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca del usuario, pudiendo esta información referirse tanto a su nombre y apellidos como a la empresa en que trabaja o su país de residencia, o no (caso de caracteres numéricos, acrónimos, etc.), pueden identificar al titular de la cuenta, debiendo dicha dirección en consecuencia considerada como dato de carácter personal.[ii]

En relación al correo electrónico dentro del derecho protección de datos conforme inicialmente se expresó en el Art. 12 de la Declaración Universal de los Derechos del Hombre de 1948 y otras regulaciones en el tiempo.[ii] El primero a destacar es su consideración como dato personal[ii], ya que el mismo puede usarse para identificar, contactar o localizar a una persona en concreto[ii], sin embargo, aflora otra inquietud poniendo estableciendo el símil de un domicilio físico, sobre éste yo tengo un título jurídico para establecerlo como propio, incluso en el caso del arrendamiento, sobre el cual, las condiciones de temporalidad y derechos existe, y en el correo electrónico solo tengo un derecho de uso, cuando más una licencia.

De la Comunidad Económica Europea: La Directiva 2000/31/CE se refiere al correo electrónico en dos artículos: comunicaciones comerciales (art. 6 de la sección 2ª) y el spam, manteniendo la legislación específica sobre contratación a distancia (Directiva 97/7/CE) y la relativa a datos personales y protección de la intimidad en materia de telecomunicaciones (Directiva 97/66/CE), La Ley Colombiana de Comercio Electrónico y el Decreto-ley 1204 de Venezuela y los

Códigos Civiles y Mercantiles sobre mensaje de Datos y Firmas Electrónicas que siguen los lineamiento de la Ley Modelo de la CNUDMI sobre comercio electrónico por lo que hace a la contratación[ii].

Dos elementos finales a considerar, el primero está relacionado precisamente con la problemática legal existente respecto de un derecho humano, y el otro con la casi omisa regulación jurídica para el correo electrónico, por lo que la primera sugerencia versa sobre la formulación de un marco jurídico basado además de lo ya indicado por la aclaración respecto de la titularidad del mismo, las normas para su contratación y un mínimo de disposiciones contenidas en los términos y condiciones, bajo los cuales se presta el servicio de acuerdo a los derechos y obligaciones que existen en toda relación jurídica, al respecto se presentó una iniciativa en Argentina que tal vez es corta en cuanto al alcance inicial, sin embargo presenta una buena representación de manifestado bajo el nombre de "Anteproyecto de Ley de Protección del Correo Electrónico (Secretaría de Comunicaciones).

El segundo corresponde al primer eslabón de análisis ya que como se ha indicado en éste trabajo, más allá de la necesaria adecuación del marco jurídico, existe en todos los aspectos prácticos de la red, por lo que el alcance es ambiciosa al decir que el correo electrónico es un dato personal, forma parte de la esfera de los derechos humanos y es usado para comunicarse, aun cuando podemos conocer a la persona atrás de la computadora que lo opera, por lo que presento la posibilidad de que se convierta en una nueva herramienta que permita llevar a cabo una identificación y autenticación legal

para el mundo virtual, en el que evidentemente alguien deberá avalar dicha identificación, tal como ya realiza para efectos fiscales en algunos países en ellos México, mediante la utilización de biometrías ligadas en certificados digitales a un esquema de firmas electrónicas avanzadas como lo presenta la legislación de UNCITRAL.

Las redes sociales como medios de información y comunicación

Mariliana Rico Carrillo[ii]

1. Las redes sociales y los derechos fundamentales como nuevo paradigma del Derecho y la Justicia

El desarrollo y crecimiento de las redes sociales en Internet (RSI) ha sido notable en los últimos años, como también lo han sido los problemas jurídicos que se presentan en ese ámbito. La utilidad de estos espacios ha traspasado su propósito original, orientado a facilitar la interrelación social, hasta transformarse en instrumentos aptos para la divulgación de información, promoción de empresas, productos y servicios profesionales, desarrollo de campañas electorales, entre otros.

Las actividades que se desarrollan en este ámbito representan un nuevo paradigma entre el Derecho y la Justicia, particularmente en lo que respecta a la protección y al ejercicio de los derechos fundamentales. En muchos casos, las redes sociales han llegado a sustituir a los tradicionales medios de comunicación como mecanismos para el ejercicio del derecho a la información y la libertad de expresión, lo cual a su vez representa un desafío en cuanto a la protección de estos derechos. La participación de los usuarios como protagonistas y como narradores de información ha acarreado penas restrictivas de la libertad en algunos países donde la información que se transmite a través de los tradicionales medios de comunicación es objeto de censura previa, tal como ha ocurrido en Venezuela con motivo de las protestas en contra del gobierno durante el primer cuatrimestre de este año.

En el presente trabajo se pone de manifiesto la utilidad de las RSI como medios de difusión de información y como instrumentos aptos para el ejercicio de la libertad de expresión y el derecho a la comunicación.

2. Libertad de expresión y derecho a la información en las redes sociales

El artículo 19 de la Declaración Universal de los Derechos Humanos (DUDH), aprobada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948[ii], proclama la libertad de expresión y el derecho a la información al indicar que todo individuo tiene derecho *"… a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."*

La libertad de expresión y el derecho a la información se encuentran íntimamente relacionados en el entendido que la libre expresión de las ideas y opiniones permite la difusión de la información en los distintos niveles de la sociedad, constituyendo un elemento fundamental en la formación de la opinión pública. Las RSI representan el canal idóneo para el ejercicio del derecho a la información en su doble dimensión (derecho a informar y ser informado), en el sentido que no sólo permiten acceder a la información de manera instantánea sino también difundirla de la misma manera, a través de la narración de los propios protagonistas de los sucesos (periodismo ciudadano)[ii].

Si bien es cierto que Internet y en particular las redes sociales representan el escenario ideal para la libre expresión de ideas y la difusión de información, el ejercicio de estos derechos en las RSI plantea toda una serie de retos y desafíos, ya que en estos entornos son los propios usuarios quienes publican y a su vez comentan información de diversa índole, sin ser conscientes que esto puede afectar los derechos fundamentales de otras personas, tal como sucede con el derecho a la intimidad, el respeto al honor y a la imagen, y la protección de datos de carácter personal, entre otros.

Entre las actividades más frecuentes que afectan estos derechos se encuentra la publicación de fotografías y videos -sin el consentimiento de la persona que figura en ellos- y la publicación de frases ofensivas que atentan contra la reputación del afectado o los afectados. Las funcionalidades técnicas de estas plataformas permiten a los usuarios no sólo publicar fotografías sino también colocar etiquetas con los nombres de las personas que aparecen en la foto. Estas actividades en la mayoría de los casos se hacen sin el consentimiento del afectado (tanto la difusión de la imagen como el etiquetado) constituyendo una violación a la privacidad, a la protección de la imagen y en algunos casos al derecho al honor de las personas[ii], con las correspondientes responsabilidades civiles y penales que estas conductas acarrean.

Ante esta situación, es conveniente recordar que la libertad de expresión y el derecho a la información, aunque son derechos inalienables no son

derechos irrestrictos. Su ejercicio está sujeto a la responsabilidad derivada del respeto a los derechos de los demás, en particular la reputación, la protección de la seguridad nacional, el orden, la salud y la moral pública. La restricción al ejercicio de estos derechos encuentra su límite precisamente en la protección de otros derechos fundamentales como el derecho a la intimidad, el honor y la propia imagen. En estos casos, es importante la ponderación entre la violación y el castigo aplicado; a la hora de aplicar una sanción hay que tener en cuenta el principio de proporcionalidad como medida de restricción a la libertad de expresión.

El principal problema que aquí se presenta está relacionado precisamente con la desproporcionalidad de la pena aplicada ante un supuesto de ejercicio abusivo de la libertad de expresión, tal como sucedió en Colombia con el famoso caso de Nicolás Castro, quien amenazó al hijo del Presiente Uribe a través de una publicación en *Facebook*[ii] y en Venezuela con las detenciones arbitrarias de distintos sujetos que ejercieron su derecho a la libertad de expresión al publicar en *Facebook*, *Twitter* y *Youtube* videos y fotografías de las protestas sociales de 2014, quienes fueron posteriormente acusados de instigación a delinquir. En estos procesos, el tipo penal aplicado (instigación a delinquir) y el castigo (privación de la libertad) son considerados desproporcionales en relación con los contenidos publicados y el supuesto ejercicio abusivo de la libertad de expresión.

Otro caso que conmocionó a la población venezolana y a la comunidad internacional relacionado con la restricción de la libertad de expresión en las RSI se presentó luego de la detención arbitraria de la juez María Lourdes Afiuni, quien fue sometida a privación de su libertad en un proceso violatorio a sus derechos humanos por otorgar la libertad condicional a un sujeto acusado de evasión de los controles de divisas. Finalmente y por presiones de los organismos internacionales defensores de los derechos humanos (Naciones Unidas y la Comisión Interamericana de Derechos Humanos) la juez fue puesta en libertad con la orden de restringir su participación en la red social *Twitter*, lo cual representa una violación flagrante a su derecho a la libertad de expresión y el derecho a la comunicación[ii].

3. Principios que rigen el ejercicio de la libertad de expresión en Internet

Ante las numerosas violaciones relacionadas con la libertad de expresión en Internet y el exceso en la imposición de sanciones derivadas de su ejercicio, los relatores especiales de los organismos internacionales que se encargan de la protección de este derecho, a saber: Naciones Unidas (ONU), la Comisión Interamericana de Derechos Humanos (CIDH), la Organización de Estados Americanos (OEA), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), firmaron en 2011 la Declaración Conjunta sobre la Libertad de Expresión en Internet (DCLEI)[ii] donde se establecen los principios aplicables a la libertad de expresión en este entorno, aplicables obviamente a las RSI. Las bases de este documento se refieren a los siguientes principios:

1. Aplicación a Internet de los mismos principios que rigen la libertad de expresión en los tradicionales medios de comunicación. En relación con las restricciones a la libertad de expresión en este entorno "…solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad."

2. Ponderación del principio de proporcionalidad como medida de restricción a la libertad de expresión en Internet, *"…en atención al impacto que dicha restricción podría tener en la capacidad de Internet para garantizar y promover la libertad de expresión respecto de los beneficios que la restricción reportaría para la protección de otros intereses.*

4. Atribución de responsabilidad sobre contenidos ilícitos, tomando en consideración *"…la aplicación de enfoques alternativos y específicos que se adapten a las características singulares de Internet, y que a la vez reconozcan que no deben establecerse restricciones especiales al contenido de los materiales que se difunden a través de Internet*.

5. Exoneración de responsabilidad a los intermediarios por los contenidos generados por terceros, siempre que no intervengan específicamente

en dichos contenidos, ni se nieguen a cumplir las órdenes judiciales que exijan su eliminación, cuando estén en condiciones de hacerlo.

En relación con el bloqueo obligatorio de sitios web, donde se mencionan específicamente las redes sociales, la DCLEI declara expresamente que esta situación *"…constituye una medida extrema—análoga a la prohibición de un periódico o una emisora de radio o televisión— que solo podría estar justificada conforme a estándares internacionales, por ejemplo, cuando sea necesaria para proteger a menores del abuso sexual".*

Finalmente, consideramos necesario destacar que las bases de la DCLEI también imponen a los Estados la obligación de promover el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión, indicando que *"…el acceso a Internet también es necesario para asegurar el respeto de otros derechos, como el derecho a la educación, la atención de la salud y el trabajo, el derecho de reunión y asociación, y el derecho a elecciones libres.".*

4. Las redes sociales como medios de comunicación e información

En Venezuela, el control de los medios de comunicación se ha convertido en una práctica usual. La censura y la salida del aire de diversos canales de radio y televisión obedecen a razones políticas. El cierre de Radio Caracas Televisión marcó un hito en la historia de los medios de comunicación en este país.

La modificación de las leyes y la intromisión del Ejecutivo Nacional con el objeto de controlar los medios de comunicación están presentes cada vez que se trata de difundir información a los ciudadanos sobre la situación del país. Esta censura se ha extendido a la información que circula a través de Internet, gracias a la modificación de la Ley de responsabilidad social en radio y televisión[ii]. El articulado de esta ley es vago e impreciso y permite sancionar a los proveedores de servicios de radio, televisión e Internet cuando difundan mensajes que fomenten "zozobra" en la ciudadanía, "alteren el orden público", o aquellos que "inciten o promuevan el incumplimiento del ordenamiento jurídico" (Art. 27). La redacción imprecisa de esta norma permite la **interpretación discrecional al momento de su aplicación, a tal** punto que en los últimos años, al amparo de esta disposición, ha sido frecuente el cierre de distintos medios de comunicación y el bloqueo de diversos sitios web que publican información que al gobierno no le conviene que sea objeto de difusión, en flagrante contradicción con los principios de la DCLEI.

En noviembre de 2013[ii] el gobierno, a través de la Comisión Nacional de Telecomunicaciones (CONATEL), determinó la responsabilidad de algunos proveedores de servicio de Internet por los contenidos difundidos y les ordenó bloquear las páginas que informaban la cotización del dólar paralelo. En relación con esta situación, cabe recordar que uno de los principios de la DCLEI establece que los proveedores de servicio de Internet no serán responsables

por contenidos generados por terceros *y que se difundan a través de estos servicios.*

Desde que comenzaron las protestas sociales en febrero de 2014, han sido frecuentes las limitaciones y bloqueos al acceso de los contenidos publicados en Internet, al extremo que el servicio fue suspendido en diversos estados del país, impidiendo a la población no sólo la posibilidad de acceder a la información sino también limitando su derecho a difundirla, en contradicción con los principios que protegen la libertad de expresión y el derecho a la información. Cuando el servicio fue restituido, se procedió al bloqueo de diversas páginas web que difundían información veraz sobre las protestas, tal como sucedió con NTN24[ii]. Estos hechos demuestran una vez más las violaciones a los principios de la DCLEI, toda vez que de acuerdo con este documento (suscrito por los principales organismos protectores de los derechos humanos), la limitación a la libertad de expresión *en Internet* **debe establecerse por ley, de manera clara y precisa,** *ser proporcionada a los fines legítimos perseguidos y basarse en una decisión judicial fruto de un proceso contradictorio.* En relación con el bloqueo de sitios web, la DCLEI declara expresamente que esta situación *"…constituye una medida extrema…que solo podría estar justificada conforme a estándares internacionales",* y respecto de la suspensión del servicio, recordemos la obligación de los Estados de promover el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión.

Las actuaciones arbitrarias del gobierno y la limitación de los distintos espacios públicos han destacado la importancia de las RSI como herramientas de comunicación y acceso a la información**.** Como hemos podido observar, los sucesos acaecidos a principios del año 2014 en Venezuela llevaron al gobierno a tomar medidas extremas con el objeto de restringir -aun más- el derecho a la información y la libertad de expresión de los ciudadanos. Ante esta situación, la población comenzó a utilizar las redes sociales como medios de comunicación e información (a objeto de informarse y difundir información) donde los narradores de las noticias eran sus propios protagonistas.

La población, haciendo uso de su derecho fundamental a la libertad de expresión y el derecho a la información no encontró otra forma de comunicarse que los canales que ofrecen las redes sociales. Es de destacar que también ha habido actuación arbitraria y represiva del gobierno en este ámbito. El Ejecutivo, consciente de la importancia de estos espacios procedió a bloquear parte del contenido publicado (principalmente videos y fotografías). También se observaron diversas detenciones por la difusión de información en las RSI[ii]. En el estado Táchira fue notable el caso de dos individuos que fueron imputados por "retuitear" mensajes que otro emisor publicó en esta red social, quedando sometidos al régimen de presentación. Durante los meses de marzo y abril también fueron emitidas diversas órdenes de allanamiento con la finalidad de incautar computadoras portátiles, celulares y otros objetos para poder determinar presuntos ilícitos contemplados en la Ley contra Delitos Informáticos e imputar la comisión de delitos por la utilización de las RSI[ii].

En la actualidad las RSI tienen un altísimo nivel de penetración en Venezuela, su importancia como medios de comunicación e información es tal que el gobierno ha intentando regular y controlar la participación de los venezolanos en estos espacios. En febrero de 2014, CONATEL amenazó con castigar a los medios que hicieran apología de la violencia en la cobertura de las protestas sociales, incluyendo la información publicada en Internet y en las RSI[ii] . El 13 de marzo de este mismo año, CONATEL se reunió con los proveedores de Internet para intentar censurar el contenido noticioso que afectara la imagen del gobierno pretendiendo restringir el acceso a *Twitter* y *Youtube*[ii]. Durante el mes de junio, el presidente de la Comisión de Comunicación de la Asamblea Nacional, propuso un debate sobre el uso de las redes sociales en Venezuela y desarrollar, mediante una ley, el artículo 60 de la Constitución, que plantea limitar el uso de la informática. En opinión de los expertos, el verdadero objeto de esta ley no sería otro que *"el de limitar y restringir el uso de las redes sociales en el país, así como penalizar su contenido al momento de expresar críticas o hacer señalamientos al Gobierno y a sus personeros"*[ii]

5. Consideraciones finales

Es evidente que en Venezuela la única ventana abierta a la libre expresión son las redes sociales. La participación de los usuarios en este tipo de espacios facilita la difusión de la información y permite la formación de la opinión pública a través de la publicación de noticias y sus respectivos comentarios.

En el marco de las protestas sociales de 2014, las RSI se convirtieron en protagonistas esenciales, toda vez que permitieron a la población difundir, comentar y compartir la información que los medios de comunicación se negaron a transmitir (en el caso de los medios cercanos al gobierno) o se vieron imposibilitados de hacerlo, debido a la excesiva regulación que existe en este entorno (en el caso de los medios privados).

Las circunstancias descritas ponen de manifiesto el papel que desempeñan las RSI como medios de comunicación e información, su importancia es tal, que en la actualidad son consideradas como "las grandes aliadas de la verdad y de la información objetiva y veraz, así como la herramienta de comunicación y opinión más directa de los ciudadanos". Gracias a las redes sociales, la población puede comunicarse y obtener información sobre los niveles de inflación, el desabastecimiento, la devaluación, el alto costo de la vida, la pérdida del valor adquisitivo de la moneda, los niveles de pobreza y desempleo, entre otros aspectos que afectan severamente al pueblo venezolano[ii].

A pesar de la intención del Ejecutivo de regular y controlar estos espacios, la restricción en el acceso y participación de las RSI puede convertirse en un arma de doble filo y acarrear consecuencias negativas graves para el propio gobierno, ya que avalaría -una vez más- las acusaciones de totalitarismo,

violación a los derechos humanos y ataques a la libertad de expresión que tanto se han denunciado internacionalmente[ii].

PONENCIA PARA EL XVIII CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA A CELEBRARSE EN SAN JOSE DE COSTA RICA

TEMA: *"*RESPONSABILIDADES CIVILES DE LOS ISP DERIVADAS DE INTERNET*"*

AUTOR: HORACIO FERNANDEZ DELPECH [ii] - ARGENTINA

1. Introducción

La temática de las responsabilidades civiles derivadas de Internet es de trascendental importancia, tanto por la falta de una legislación a su respecto en casi toda América Latina, así como por una serie de causas judiciales que se están tramitando en la Republica Argentina.

En esta ponencia intentaré analizar el tema de las Responsabilidad civiles que pueden resultar para los ISP por sus actividades en Internet, en el marco del nuevo paradigma de la justicia y el derecho.

A tal fin debemos precisar primero que se entiende actualmente por ISP, o Internet Servicie Provider, en la usual terminología en ingles.

Tal como lo he analizado en otras oportunidades [ii], además de los **usuarios de Internet,** que son aquellas personas que acceden a un sitio de la red para buscar información o utilizar alguna de las diferentes aplicaciones que la red brinda, y de los **proveedores de contenido,** que son todos aquellos autores, editores o simplemente usuarios que proveen información a los sitios de Internet [ii] , existen los **Proveedores de Servicio de Internet . Internet Service Providers . ISP**, que son quienes posibilitaban la conexión entre el usuario y los contenidos incorporados al sito y que conforme la actual doctrina internacional podemos dividirlos en:

- **Los Proveedores de Acceso . Internet Access Providers . IAP**. Son quienes brindan a los usuarios individuales el servicio de conexión con la red Internet, a través de un server de gran poder conectado a la red (nodo), a fin de poder llegar así a los diferentes sitios de la red. Por su

parte el proveedor de contenido creador de una página o sitio, requiere también los servicios de estos proveedores de acceso a fin de poder incorporar su sitio a la red.

- **Los Proveedores de Alojamiento . Hosting Service Providers**. **HSP**. Son quienes brindan el servicio de alojamiento de páginas Web en su propio servidor así como otros servicios adicionales.
- **Los Proveedores de Red . Networks Service Providers**. **NSP**. Son quienes brindan una estructura técnica (líneas telefónicas, de cable o por antena), a fin de que el usuario se conecte a través del Proveedor de Acceso con la página o sitio almacenada por el Proveedor de Alojamiento. De esta forma se completa el circuito en el que el usuario individual accede a los contenidos incorporados por el Proveedor de Contenidos.

  Es de resaltar que muchas veces existen empresas que brindan conjuntamente los servicios de Proveedor de Acceso a Usuarios y Proveedor de Alojamiento, e incluso actúan en algunos casos también como proveedores de Red.

- **Los proveedores de servicios de aplicaciones. Aplication Service Provider . ASP.** Sus funciones consisten fundamentalmente en habilitar software u otras aplicaciones informáticas en Internet, de manera que pueda ser utilizado por los clientes sin necesidad de instalarlo en sus computadores. Es decir, el cliente accede a las aplicaciones utilizando únicamente su browser. La información se almacena en un Data Center que tiene todas las características de seguridad necesarias. Este servicio básico se complementa con otros servicios adicionales, como la

administración de infraestructura (bases de datos, computadores centrales, usuarios, etc.), el manejo de respaldos y recuperación, la ejecución de procesos, y todos aquellos servicios que garanticen una explotación cómoda, continua y segura. Este sujeto tiene una gran similitud con el proveedor de cloud computing.

Pero ya hace algunos años aparece un quinto sujeto, al que se lo comienza a incluir entre los Proveedores de Servicio ISP (Internet Service Providers), y nos referimos a los **Proveedores de Localización**, y para expresarlo mas claramente estamos hablando de los buscadores de Internet, que son quienes nos facilitan hoy en día la búsqueda y conexión con determinados sitios.

Lo que voy a intentar tratar ahora es ver cuales son las responsabilidades que les pueden caber a estos Proveedores de Servicio de Internet (IAP, HSP, NSP, y ASP), por los contenidos que transmiten, y a los Proveedores de localización por los resultados de las búsquedas de los usuarios, cuando tanto esa transmisión o ese resultado de búsqueda contiene contenidos nocivos, ilícitos o que causan daño.

2. Libertad de Contenidos en Internet

Internet nace como un ámbito de plena libertad en donde pareciera que todo es valido y en donde cualquier intento de filtrar, impedir o castigar por contenidos violatorios de la moral o de la ley no es aceptado.

En todas partes del mundo existe desde hace ya años esa conciencia de plena libertad en Internet fundamentalmente garantizando de esta forma la plena libertad de expresión.

La Constitución de la Republica Argentina garantiza ampliamente la libertad de expresión y, tanto los Convenios Internacionales suscriptos por la Argentina, como la jurisprudencia de nuestra Corte Suprema, establecen una prohibición a la censura previa de los contenidos, aún cuando con ellos se cometiera un delito.

Pero el derecho a la libertad de expresión no es un derecho absoluto, y tiene ciertas restricciones cuando se trata de contenidos ilícitos o prohibidos por la ley.

Tanto la doctrina como la jurisprudencia nacional e internacional han admitido el establecimiento de restricciones sobre el derecho de libertad de expresión con el fin de proteger a la comunidad de ciertas manifestaciones ofensivas y para prevenir el ejercicio abusivo de ese derecho.

Pero esas restricciones a la libertad de expresión no pueden consistir en censurar previamente el contenido, pero sí en establecer su prohibición o ilicitud, y en caso de darse el supuesto, de juzgar con posterioridad al acto la responsabilidad que puede caber.

Igual situación se da en los contenidos que causan un daño, en los cuales es valido pensar en el juzgamiento con posterioridad al acto de la responsabilidad que puede caber.

En estos casos debemos ver cual es la responsabilidad que puede tener cada uno de los actores que intervienen en la incorporación y transmisión de ese

contenido que pueden resultar responsable con posterioridad al acto, en lo que ha dado en llamarse "*responsabilidad ulterior*".

En la Republica Argentina, el art. 14 de la Constitución Nacional consagra el derecho a publicar las ideas por la prensa sin censura previa, garantizando así ampliamente la libertad de expresión.

Asimismo existen normas legales que hacen extensivo dicho derecho a Internet, [ii] y, tanto los Convenios Internacionales suscriptos por la Argentina, como la jurisprudencia de nuestra Corte Suprema, establecen una prohibición a la censura previa de los contenidos, aún cuando con ellos se cometiera un delito.

Destaco que el concepto de "idea" de nuestra carta magna se ha hecho extensiva, tanto en la doctrina como en la jurisprudencia Argentina (al igual que en la totalidad de los documentos internacionales), a las informaciones e ideas de todo tipo.

La Corte Suprema ha establecido que: "*no todo lo que se difunde por la prensa o se emite en programas radiales o televisivos o por cualquier otro medio goza del amparo otorgado por la prohibición a la censura previa, sino aquello que por su contenido encuadra en la noción de información o difusión de ideas*" [ii]

La Jurisprudencia Argentina ha sido muy fiel a este principio y ha establecido que no corresponde la censura previa ni aún en el caso de que la publicación implique la comisión de un delito, estableciendo claramente que en ese supuesto sólo es posible juzgar las responsabilidades con posterioridad al acto pudiendo imponerse incluso penas en caso de delito. (caso Verbitzky)

3. Doctrina de las Responsabilidades Ulteriores

Pero el derecho a la libertad de expresión no es un derecho absoluto, y tiene ciertas restricciones cuando se trata de contenidos ilícitos o prohibidos por la ley.

Tanto la doctrina como la jurisprudencia nacional e internacional han admitido el establecimiento de restricciones sobre el derecho de libertad de expresión con el fin de proteger a la comunidad de ciertas manifestaciones ofensivas y para prevenir el ejercicio abusivo de ese derecho.

Pero esas restricciones a la libertad de expresión no pueden consistir en censurar previamente el contenido, pero sí en establecer su prohibición o ilicitud, y en caso de darse el supuesto, de juzgar con posterioridad al acto la responsabilidad que puede caber. En estos casos el autor de la incorporación de ese contenido puede resultar responsable con posterioridad al acto, en lo que ha dado en llamarse ***"la doctrina de las responsabilidades ulteriores"*.**

Hasta hace no muchos años eran escasos las situaciones en que se debía juzgar responsabilidades de este tipo.

En una Web en que el usuario solamente bajaba contenidos de Internet, los problemas eran menores, pero ya desde comienzos del nuevo siglo, Internet se transforma en algo mucho mas activo. La nueva Internet 2.0, es una Internet interactiva donde todos ingresamos contenidos que a veces rozan derechos, cuando no los afectan. Entonces nos encontramos frente a un choque de derechos y nos preguntamos: ¿podemos censurar esos contenidos?

La apología del delito, la propalación de injurias y calumnias, las propagandas discriminatorias, la violación y afectación de la intimidad y de la privacidad de las personas, las violaciones a los derechos propiedad intelectual, entre otras cuestiones. son ahora situaciones frecuentes en Internet y requieren entonces una respuesta de los regímenes jurídicos mas allá de ese principio de la libertad en Internet.

Como dijera, nuestra Constitución e incluso normas internacionales impiden la censura previa. Pero necesitamos encontrar un equilibrio, ya que la libertad de unos termina donde comienza la libertad de otros.

La doctrina de las responsabilidades ulteriores podría resumirla indicando que implica que cada uno puede escribir, publicar, subir o transmitir contenidos en base a la libertad de expresión garantizada por la Constitución, y si estos contenidos resultaren ser difamatorios, ofensivos o lesivos a los derecho de otro o configuren un ilícito, será posteriormente la Justicia quien determine la responsabilidad de la persona y en su caso el resarcimiento económico por los daños y perjuicios ocasionados.

Esta doctrina que fue formulada, para la prensa escrita, por la Convención Americana sobre Derechos Humanos (Art. 13) [ii] y otros Convenios Internacionales, y que tuvo acogida en numerosos fallos de la Corte Suprema de Justica de la Argentina, así como en la principal jurisprudencia americana, creo que sin duda es plenamente aplicable a Internet.

Internet es libre, pero ello no se puede traducir una total impunidad para quien viola la ley o causa daños a terceros.

Con relación a lo estipulado en el art. 13 referido, la Comisión Interamericana de Derechos Humanos, ha dicho también:

"*La Convención permite la imposición de restricciones sobre el derecho de libertad de expresión con el fin de proteger a la comunidad de ciertas manifestaciones ofensivas y para prevenir el ejercicio abusivo de ese derecho. El artículo 13 autoriza algunas restricciones al ejercicio de este derecho, y estipula los límites permisibles y los requisitos necesarios para poner en práctica estas limitaciones. El principio estipulado en ese artículo es claro en el sentido de que la censura previa es incompatible con el pleno goce de los derechos protegidos por el mismo. La excepción es la norma contenida en el párrafo 4, que permite la censura de los "espectáculos públicos"* para la protección de la moralidad de los menores.

La única restricción autorizada por el artículo 13 es la imposición de responsabilidad ulterior. Además, cualquier acción de este tipo debe estar establecida previamente por la ley y sólo puede imponerse en la medida necesaria para asegurar: a) el respeto de los derechos o la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

4. Legislaciones Europeas y Norteamericana

La **"Multimedia Acto**" dictada en Alemania en el año 1997, establece diferentes tipos de responsabilidades según sea la clase de Proveedor de Servicio de Internet de que se trate, distinguiendo para ello a tres tipos de proveedores: "Information Providers", "Hosting Providers" y "Access Providers".

Con relación al “Information Providers”, se establece la plena responsabilidad por los contenidos que incorpora al sito; mientras que con relación a los “Access Providers” y “Hosting Service Providers” se determina que son responsables sólo si tienen conocimiento de los contenidos y teniendo en cuenta si tomaron las medidas técnicas adecuadas frente a tal conocimiento.

En la Comunidad Europea, la **Directiva de Comercio Electrónico del Parlamento Europeo** [ii], establece en el art. 12 la falta de responsabilidad de los ISP, al disponer:

> *“No serán responsables por los datos transmitidos a menos que: hayan originado o modificado ellos mismos los datos o hayan seleccionado a éstos o a sus destinatarios”.*

Con total acierto Miguel Peguera Poch, comentando la Directiva 2000/31/CE, nos dice: *“…El hecho de que los contenidos que el ISP transmite o almacena hayan sido proporcionados por terceros, esto es, que sean contenidos ajenos, resulta esencial desde la perspectiva de la exención de responsabilidad. Así, cuando el prestador de servicios coloca en la red o transmite contenidos propios, la exención de responsabilidad pierde su razón de ser. En efecto, la exención se funda en que el prestador del servicio intermediario no ha tenido parte ni en la creación ni en la decisión de transmitir o de hacer accesibles los contenidos ilícitos y potencialmente dañinos: ha sido un tercero quien lo ha hecho. A ello se añade la idea de que no le es técnicamente posible, o bien le resulta excesivamente costoso, supervisar lo que circula por sus redes o se aloja*

en su servidores, con lo que normalmente ni siquiera tendrá conocimiento de los contenidos concretos, y aún menos de su carácter lícito o ilícito". [ii]

Se completa este principio de la irresponsabilidad de los ISP con lo dispuesto en el art. 13 de la Directiva europea sobre la memoria tampón o caching [ii] y en el art. 14 sobre los supuestos de hosting.

El artículo 13 establece que:

> *" Cuando se preste un servicio de la sociedad de la información consistente en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio y que implique su almacenamiento automático, provisional y temporal, realizado con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios del servicio, a petición de éstos, no será responsable por el contenido de la transmisión, (almacenamiento automático, provisional y temporal) siempre que el prestador a) no modifique la información. b) Cumpla las condiciones que permitan el acceso a ella. c) Respete las normas relativas a la actualización de la información. d) No interfiera en la utilización lícita de tecnología, con el fin de obtener datos sobre la utilización de la información". e) Retiren la información que hayan almacenado, o hagan imposible el acceso a ella, en cuanto tengan conocimiento efectivo de que ha sido retirada del lugar de la red en que se encontraba inicialmente o que se ha imposibilitado el acceso a ella o que un tribunal o autoridad administrativa competentes han ordenado retirarla o impedir que se acceda a ella".*

En lo referente al alojamiento de datos ("hosting"), el art. 14 de la Directiva dispone que:

> *"Los prestadores de un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio no serán responsables del contenido de los datos almacenados a petición del destinatario, siempre que no tengan conocimiento efectivo de que la actividad o la información a las que afecte es ilícita y, en lo que se refiere a una acción de daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele la existencia de una información ilícita, y no actúa con prontitud para retirar esos datos".*

En España, la **Ley de servicios de la sociedad de la información y de comercio electrónico** [ii] , trata detalladamente el tema refiriéndose en los arts. 13 a 17 a la responsabilidad de los prestadores de los servicios de la sociedad de la información distinguiendo entre ellos a:

- los operadores de redes y proveedores de acceso a una red de telecomunicaciones;
- los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios;
- prestadores de servicios de alojamiento o almacenamiento de datos;
- prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda; Resalto que la ley española incorpora entre los ISP a los intermediarios de localización.

Todos estos son, en la terminología habitual y que referimos en el comienzo del capitulo anterior, Proveedores de Servicio de Internet.

En los tres primeros casos la ley española exime de responsabilidad a estos prestadores salvo casos excepciones como ser que hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos.

En el cuarto caso, de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda, y que incluye a los proveedores de localización (buscadores de Internet), la ley es mas rigurosa y establece expresamente:

> *" Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:*
>
> - *a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o*
> - *b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.*
>
> *Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador*

conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.“

En EE.UU. la temática de la libertad de los contenidos en Internet y la responsabilidad de los proveedores de servicio ha sido objeto de un amplio debate.

En 1996 se dictó en el marco de la ley de telecomunicaciones la **“Communications Decency Act” (CDA**), la que fue ratificada como ley federal el 8 de Febrero de 1996. Esta ley establecía responsabilidades penales a quienes transmitiesen vía Internet material obsceno o indecente destinado a menores.

De inmediato el Acta fue impugnada judicialmente por la Asociación de Libertades Civiles de EE.UU.(American Civil Liberites Union), sosteniendo dicha Asociación que el acta era inconstitucional por violar la libertad de expresión consagrada por la Constitución Norteamericana, obteniéndose que en el Distrito de Filadelfia la justicia decretase la no aplicación de la normativa del acta.

La fiscal Reno también recurrió contra el acta, y el caso llegó a la Corte Suprema en donde el 26 de Junio de 1997, en un fallo no unánime (7 votos contra 2), con fundamento en la Primera Enmienda de la Constitución Norteamericana, se declaró su inconstitucionalidad [ii].

Se consideró allí que el acta al imponer restricciones a la difusión por Internet de material sexual, vulneraba el derecho a la libre expresión e implicaba una censura ilegal.

Se expresó también en el fallo: *"...a pesar de la legitimidad y la importancia de la meta legislativa de proteger a la niñez de los materiales peligrosos, coincidimos en que el estatuto limita la libertad de expresión y en que el Gobierno no tiene la potestad para discriminar a los adultos con materiales que no sean aptos para niños".*

Como consecuencia del citado fallo el entonces Presidente Clinton se refirió públicamente al tema propiciando la necesidad de encontrar una solución técnica que permitiese proteger a los menores de edad sin que ello violase la libertad de expresión.

El Congreso de los EEUU, por iniciativa de la Senadora Patty Murray promulgó entonces en Octubre de 1998, el **Acta para la Protección o Seguridad en Línea de la Privacidad de los Menores.**

Allí se contempla el uso de programas filtro o de selección de contenidos por parte de los padres, estableciendo que los operadores de sitios deben exhibir notas al respecto.

Desde entonces la jurisprudencia norteamericana ha eximido de responsabilidad a los ISP. Tal los casos "Lunney vs. Prodigy Service" (de Diciembre de 1999) y "Ben Ezra, Weinstein & Co. Inc. vs American OnLine" (de Marzo de 2000), en donde se determinó que las empresas demandadas que

eran Proveedores de Servicio no eran responsables, ya que sólo tenían calidad de distribuidores o editores secundarios.

Finalmente la **Digital Millennium Copyright Act (DMCA)** , aprobada en EE.UU en Octubre de 1998, modificó la Copyright Act en diversos puntos, figurando entre ellos la incorporación de la Sección 512 que regula la limitación de la responsabilidad en línea de los servidores de Internet (ISP).

La normativa libera de responsabilidad a los ISP por:

- la mera transmisión de contenidos (transient host).
- el almacenamiento de contenidos, de manera que permita al servidor reducir tanto el tiempo de transmisión a sus usuarios como su ancho de banda (system o proxy caching).
- el almacenamiento de contenidos en sistemas o redes bajo la dirección de los usuarios (hosting)
- el uso de mecanismos de localización de la información a través de los cuales se dirige a los usuarios a contenidos infractores.

Por otra parte, establece un detallado sistema de *"notice and take down"* (detección y retirada), para hacer posible que los titulares de derechos de autor identifiquen las infracciones que se cometen a sus obras a través de Internet y lo notifiquen a los servidores afectados para que el material supuestamente infractor sea retirado o su acceso bloqueado.

La DMCA establece consecuentemente que la responsabilidad de los ISP se genera únicamente cuando la incorporación del contenido es manifiesta o habiendo sido notificado que existen contenidos violatorios de la ley, no toma de inmediato las medidas necesarias para su retiro.

Si bien la normativa de la DMCA esta referida a violaciones a los derechos de copyright, estas normas también han sido aplicadas a otros contenidos ilícitos o que cusan daño a terceros.

Vemos como este tema ha sido tratado en dos sistemas jurídicos, con dos soluciones parecidas pero no iguales.

- En la ley Española, se establece que el sitio web o el buscador es responsable recién cuando tiene conocimiento efectivo de la infracción, y que este conocimiento efectivo existe recién cuando un órgano competente haya declarado la ilicitud del acto. Así es como en España, y en Europa en general, el buscador sería responsable subjetivamente – salvo que le demostremos culpa directa– sólo cuando un órgano competente le ordene bajar ese contenido porque es ilícito o es inmoral o causa un daño y si no cumple, entonces sería responsable. Hacemos presente que conforme reciente jurisprudencia española si bien el párrafo segundo de la ley hace mención a que se entenderá que existe ese conocimiento cuando un órgano competente lo haya declarado, la coletilla final de la norma, que indica la posibilidad de "*otros medios de conocimiento efectivo que pudieran establecerse*", ha permitido al Tribunal Supremo señalar en otros casos que tanto la comunicación

remitida por el tercero afectado como la propia naturaleza de los contenidos pueden servir como medio de alcanzar ese conocimiento efectivo y por lo tanto romper la exención de responsabilidad

- En Estados Unidos la situación es distinta, la responsabilidad es más amplia. Allá funciona el sistema del *notice and take down,* establecido primero por la Digital Millenium para la propiedad intelectual y que se ha ampliado después a los ISP y buscadores de Internet directa o indirectamente:

  "*Yo le aviso que esto es una infracción; desde este momento usted es responsable si un juez lo condena*."

  Para que nazca la responsabilidad no se necesita en Estados Unidos la decisión judicial que ordene bajar el contenido, sino que basta que el afectado lo solicite, y no se efectúe de inmediato la bajada del contenido

5. Nueva legislación Brasilera y Chilena

En abril de 2014 el Brasil dictó una ley Marco de Internet, en la que se establece entre otras cosas que los ISP sólo podrán ser responsabilizados por contenidos que transmiten si hay una resolución judicial que ordena la baja y ellos no la cumplen. De esa manera, se busca evitar que las empresas tengan la potestad de definir por sí mismas cuándo un material debe ser retirado.

La ley de Propiedad Intelectual de Chile, en su modificacion dispuesta por la ley Nº 20.435, contempla la responsabilidad de los ISP pero con relacion solo

a las violaciones a la propiedad intelectual. Establece asi la ley que están exentos de responsabilidad si eliminan los contenidos infractores tan pronto tengan conocimiento de ello. Con la nueva ley, se considera que los prestadores de servicios de Internet conocen de la existencia de los contenidos que transmiten o alojan una vez que reciben una notificación judicial al respecto.

6. La Sentencia del Tribunal de Justicia de la Unión Europea del 13 de Mayo de 2014. [ii]

Si bien referido únicamente a los datos personales, la Gran Sala del Tribunal de Justicia de la Unión Europea, dictó recientemente este importante fallo, en el cual establece que, conforme la Directiva 95/46/CE, debe interpretarse que la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por ultimo ponerla a disposición de los internautas, debe calificarse como tratamiento de datos personales.

Asimismo que cuando esa información contiene datos personales, el motor de búsqueda debe considerarse responsable de dicho tratamiento, pudiendo en estos casos el afectado pedir la eliminación de dicho dato.

De acuerdo a este controvertido fallo, cualquier persona que se sienta afectada por cuanto sus datos personales aparecen mencionados en un buscador, como resultado de la indexación de una noticia sobre su persona, tiene el derecho a exigir directamente al buscador, la supresión de ese dato, sin necesidad de cumplir con ningún requisito previo, siempre que alegue que el dato sobre su personal le produce perjuicio y ya no sea pertinente por el

tiempo transcurrido, respaldando así el derecho a la autodeterminación informativa y el derecho al olvido. Sobre este tema me referí ampliamente en una nota publicada en la edición del Diario La Ley de Buenos Aires, del 9 e Junio de 2014.

Hago presente que como consecuencia de este fallo, Google ha implementado un formulario para que cualquier persona que se considere afectada e incluida en la doctrina del fallo, pueda pedir la eliminación de los datos que se refieren a su persona y que considere que sean inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, o que no estén actualizados o que se conserven durante un período superior al necesario (derecho al olvido).

7. El Régimen de responsabilidad en la Argentina. Criterios de Atribución de Responsabilidad. Responsabilidad Contractual y Extracontractual. Responsabilidad Subjetiva y Responsabilidad Objetiva

En el derecho argentino tenemos dos tipos de responsabilidad: la contractual, derivada del incumplimiento de un contrato, y la extracontractual, que se origina por haber producido un daño sin que exista un nexo contractual.

En estos casos de perjuicios a terceros por páginas de Internet o a través de buscadores, tenemos que encontrar la solución en la responsabilidad extracontractual, evidentemente. Y para que se dé esa responsabilidad, tendremos que determinar primero la existencia del daño material o moral medible y resarcible en dinero. Después debe existir una relación causal entre el daño y el hecho que dio lugar al mismo. Acá ya es más difícil: ¿existe la

relación causal? Sí, ¿pero en el buscador? Y, yo creo que también podría existir esa relación de causalidad. El hecho cuestionado debe ser antijurídico, si no hay antijuridicidad no puede darse la responsabilidad extracontractual.

Pero sentada la existencia de una responsabilidad extracontractual, debemos determinar el segundo factor de atribución de responsabilidad.

Se trata de determinar si se trata de una responsabilidad subjetiva o estamos frente a una responsabilidad objetiva.

La **responsabilidad subjetiva** está regulada en nuestro derecho por los arts. 512 y 1109 del Código Civil que establecen fundamentalmente que *"La culpa del deudor en el cumplimiento de la obligación consiste en la omisión de aquellas diligencias que exigiere la naturaleza de la obligación, y que correspondiesen a las circunstancias de las personas, del tiempo y del lugar"*, y que *"Todo el que ejecuta un hecho, que por su culpa o negligencia ocasiona un daño a otro, está obligado a la reparación del perjuicio…"*

La **responsabilidad objetiva** está regulada en nuestro derecho por los arts.

1113, 1071, 1071 bis, y complementarios del Código Civil.

Artículo 1113. "La obligación del que ha causado un daño se extiende a los daños que causaren los que están bajo su dependencia, o por las cosas de que se sirve, o que tiene a su cuidado. En los supuestos de daños causados con las cosas, el dueño o guardián, para eximirse de responsabilidad, deberá

demostrar que de su parte no hubo culpa; pero si el daño hubiere sido causado por el riesgo o vicio de la cosa, sólo se eximirá total o parcialmente de responsabilidad acreditando la culpa de la víctima o de un tercero por quien no debe responder. Si la cosa hubiese sido usada contra la voluntad expresa o presunta del dueño o guardián, no será responsable".

El texto originario de la norma regulaba dos supuestos específicos de responsabilidad: la responsabilidad genérica del principal por los daños que causaren los que están bajo su dependencia, y la responsabilidad del guardián por las cosas de que se sirve o que tiene a su cuidado.

La reforma de 1968 del Código Civil por Ley 17711 agregó la responsabilidad de los daños causados con cosas y la responsabilidad de los daños causados por el riesgo o vicio de la cosa.

Podríamos resumir diciendo entonces que en nuestro sistema jurídico Argentino, **tenemos dos factores de atribución de responsabilidad extracontractual: la responsabilidad subjetiva, clásica, tradicional, y la nueva responsabilidad que está avanzando poco a poco, que es la responsabilidad objetiva**. ¿Dónde vamos a encontrarla? ¿Podemos decir que es subjetiva, que es objetiva? La primera es la que surge de la culpa en el daño, el que causó un daño debe resarcirlo. Esa es la responsabilidad tradicional, que podríamos endilgarle quizás al ISP incluyendo al buscador si le demostramos la culpa o la intencionalidad. Por otro lado la responsabilidad objetiva –que tiene muchos defensores– es la responsabilidad sin culpa, que se crea por otros motivos, que se crea para tener respuesta ante el daño, para que ciertos actores respondan

aún sin haber cometido culpa. ¿Por qué así? Porque se ejerce una actividad riesgosa o peligrosa.

Yo creo que la responsabilidad objetiva no puede ser atribuida a Internet, porque no puede decirse que Internet sea una actividad riesgosa o peligrosa.

Me inclino rotundamente por la exclusión de Internet de este tipo de responsabilidad. Creo que Internet no es lo mismo que el fabricante de un arma o el propietario de una plataforma petrolera. Si creáramos una responsabilidad objetiva sobre Internet, además de equivocar en su origen, la estaríamos destruyendo. Sería la destrucción de un medio que ha beneficiado enormemente al mundo; el acceso al conocimiento y a la información que nos ha dado Internet no puede ser desconocido.

El concepto de actividad peligrosa o riesgosa es por su naturaleza un concepto relativo y depende del estado de avance de la ciencia y de la técnica en un sector determinado; lo que lleva a calificar de peligrosas a actividades que antes no lo eran o viceversa.

Debemos tener en cuenta que la utilización de la informática en el mundo actual ha dado lugar a múltiples usos, de los cuales algunos pueden implicar actividades peligrosas pero no así otros. Pareciera que la utilización de la informática en el manejo de los bancos de datos podría considerarse una actividad peligrosa, así como también el desarrollo de determinados software destinado a actividades industriales que son en si peligrosas, como podría ser el destinado a centrales nucleares, etc.

Bustamante Alsina, nos dice que los sistemas automatizados de información que emplean la informática, no son cosas peligrosas que dañen por sí mismas, sino instrumentos que el hombre maneja o acciona a su voluntad.

También se ha dicho que "*No hay cosas peligrosas o no peligrosas en sí, sino que la tal peligrosidad depende de una situación jurídica integrada por la cosa y la particular circunstancia en que se originó el daño".* [ii]

Tradicionalmente se ha considerado que la responsabilidad objetiva debe estar asociada con actividades que son potencialmente peligrosas y que tienen una alta probabilidad de daño. Tal el caso de la energía eléctrica, la producción o tratamiento de explosivos o materiales radioactivos.

Creo que cuando se trata de perjuicios que son causados por la cosa interviniente en forma directa , y esa cosa es un elemento de potencial peligro, podría regir el sistema de responsabilidad objetiva del artículo 1113 2º párrafo del Código Civil, pero cuando la cosa no interviene autónomamente en la producción del daño, sino respondiendo al accionar del operador, debe ser aplicado un criterio de atribución de responsabilidad subjetiva conforme al artículo 1109 del Código Civil.

¿Cuál es la naturaleza del ISP? ¿Son editores de la información? Yo creo que no, ni el que transmite técnicamente la información ni el buscador que me lleva a ella editaron la información. ellos no crean el link, se crea automáticamente con la indexación que realiza el algoritmo creado. Son sólo

distribuidores de información, reitero, no le podemos atribuir entonces una responsabilidad objetiva. Pero sí una responsabilidad subjetiva, en la medida que le podamos probar que ellos conocían el hecho, que fueron partícipes, que tuvieron culpa, que hubo negligencia de su parte.

Opino que en el estado actual de la tecnología, pese a que algunos fallos dicen lo contrario, no podemos decir que los buscadores sean per se culpables por los contenidos que indexan. Su culpabilidad puede surgir en el momento que son advertidos de la circunstancia dañina, que es más o menos lo que han dicho los últimos fallos. La posición internacional dice que son meros distribuidores de información, tienen responsabilidades subjetivas por las infracciones de terceros, porque hay un daño, una causalidad, y hay una acción dolosa o culposa. Tenemos que probarle la culpa por lo menos, la negligencia. ¿Cuándo nace esa responsabilidad? Por las infracciones propias serían responsables plenamente. Entonces yo diría que si los buscadores no crean la información, no tienen plena responsabilidad, sino indirecta, secundaria, que surge por la responsabilidad de un tercero.

7. La Jurisprudencia Argentina. Los casos de las modelos

En materia jurisprudencial, un caso interesante en Argentina es el conocido como ***los juicios de las modelos***.

Hace algunos años numerosas modelos argentinas y personas vinculadas al espectáculo, advirtieron que colocando sus nombres en los buscadores Google y Yazoo, se obtenían referencias vinculantes con sitios pornográficos y de

prostitución, así como se difundían sus fotografías en los buscadores de imagen. Esto provocó que muchas de estas modelos, considerándose afectadas moralmente, promovieran juicios de daños y perjuicios contra los buscadores Google y Yahoo, juicios a los que se los llamo *"los juicios de las modelos*".

Se trata de mas de 200 causas judiciales que tramitan ante los tribunales argentinos, en las cuales las modelos demandan daños y perjuicios a Google de Argentina y a Yahoo Inc. , por considerarse afectadas moralmente por citas en los buscadores referidos, que las vinculaban con la prostitución.

En esos casos, recién tenemos unas pocas sentencias, que no son coincidentes entre si.

El primer caso fue el de una integrante del grupo musical "Bandana", Virginia Da Cunha, quien en el año 2009 obtuvo a su favor la primer sentencia dictada en la República Argentina en relación a esta temática conforme el fallo dictado por la Dra. Virginia Simari, titular del Juzgado Nacional de Primera Instancia en lo Civil 75. El fundamento del fallo condenando a Google y a Yahoo fue la responsabilidad tanto objetiva como subjetiva. Posteriormente la Cámara Civil, revocó dicho decisorio, con voto dividido y rechazo la demanda. El expediente se encuentra en la Corte Suprema de Justicia de la Nación vía recurso extraordinario.

El segundo de los casos fue dictado el 4 de marzo de 2010 en la causa

promovida por la modelo Belén Rodríguez [ii] contra los mismos buscadores. En este fallo se hizo también lugar a la demanda pero condenando en base a un criterio de atribución de responsabilidad subjetiva..

En un meduloso fallo la Jueza analiza minuciosamente los hechos así como toda la doctrina nacional e internacional, fallando a favor de la actora y condenando a los demandados. Entre otros argumentos se expresa: *"Así, la conducta culpable de las demandadas, nacida -reitero- a partir de la notificación fehaciente de la afectación a los derechos personalísimos de la actora, engendra la obligación de reparar el daño causado. Tienen pues responsabilidad directa por violación al principio legal del "alteran non laedere" que el Código Civil prevé en el art. 1109, debiendo responder por las consecuencias dañosas, en tanto medie adecuado nexo de causalidad entre ésta y los daños probados (cfr. arts. 901, 905, 906, 1067, 1068, 1069 y cc del Código Civil). "*

Esta Sentencia fue apelada y la Cámara la modifico levente, lo que llevo al Recurso Extraordinario ante la Corte Suprema donde se encuentra desde hace algunos meses a Sentencia, luego de que la Corte llamara a una audiencia publica para escuchar a las partes y a los especialistas en el tema..

El tercero de los mencionados casos, el fallo de Paola Krum [ii] dictado por la Sala J de la Cámara Civil, luego de un minucioso y pormenorizado análisis del caso establece:

“ Las accionadas son titulares de sus propias páginas web o sitios y por ende responsables de los contenidos que ellos introducen o reproducen, sean por

medios automatizados o no.

c. La actividad que desarrollan los buscadores es una actividad riesgosa". Al respecto sostuvo la magistrada que *"...Resulta evidente que esta interpretación abarca no sólo a la actividad propia de las demandadas y a las cosas de las que se sirve, de las que son propietarias y/o guardianes, sino también quedan incluidas en lo que Pizarro llama "los otros posibles sujetos pasivos" en relación a los sitios de terceros que son el ámbito donde se genera el daño primigenio, luego multiplicado, potenciado y concretado en una magnitud casi inimaginable..."*

Como corolario en este punto en el que se fijaba una responsabilidad objetiva de los buscadores por ser una actividad riesgosa, la magistrada agregó que las demandadas también habían incurrido en responsabilidad subjetiva porque ninguna había cumplido en forma completa e inmediata con las medidas cautelares dictadas luego de iniciados los juicios y que ordenaban el bloqueo de los contenidos que afectaban a las modelos actora en los juicios.

Vemos que en este fallo se admite tanto la responsabilidad objetiva como la responsabilidad subjetiva, admitiéndose que ambas se pueden dar simultáneamente.

Finalmente La Sala L de la Camara Civil, en Noviembre de 2013 en autos "Solaro Maxwell, María Soledad c/ Yahoo de Argentina SRL y otro s/ daños y perjuicios" dicto un fallo en el cual condeno a las demandadas Yahoo y Google,

ya que coincidió con lo resuelto por la Dra. Mattera en el fallo de Paola Krum de la Sala J , estableciendo en consecuencia que la responsabilidad de las accionados, como titulares o guardadores de los buscadores en internet, no era subjetiva, sino que *"se trata de una actividad riesgosa y que debe analizarse desde la órbita de la responsabilidad objetiva por el riesgo que dicha actividad genera (art. 1.113 Cód. Civil). Ello por cuanto si bien los contenidos de los sitios son cargados por terceros, lo cierto es que la finalidad de los buscadores es facilitar su llegada a sus usuarios mediante su indexación".* Conforme a esta responsabilidad objetiva condeno a las demandadas.

Creemos que el camino que vamos haciendo es ése, pero que la jurisprudencia Argentina está marcando que la responsabilidad parte recién desde el momento en que el buscador es anoticiado de la infracción. Creo que no podemos llevar a condenarlo de por sí, porque el responsable es el sitio y no el buscador.

8. Intentos de dictar normativa en Argentina

Desde hace algunos años varios fueron los intentos de dictar una normativa relacionada con la responsabilidad de los ISP, pero recién el el 22 de febrero de 2011, el diputado Federico Pinedo presentó un proyecto que regula la actividad desarrollada por los ISP y que tomo estado parlamentario.

El proyecto consta de 10 artículos en los cuales se recogen principios de legislación extranjera y de la jurisprudencia local e internacional.

En particular, el Proyecto establece que los Buscadores de Internet o las Redes Sociales deben responder por contenidos publicados por terceros cuando dichos contenidos violentan derechos personalísimos tales como el honor, la imagen o la intimidad. El proyecto establece que la responsabilidad nace cuando el IOSP tiene el conocimiento efectivo de que la información almacenada viola normas legales o derechos de terceros, considerando que "tiene conocimiento efectivo" desde el momento en que es notificado del dictado de alguna orden judicial que ordene la baja o bloqueo del contenido.

En consecuencia el Proyecto Pinedo considera que no puede imputarse responsabilidad objetiva fundando la responsabilidad en un criterio de atribución de responsabilidad subjetiva. Este Proyecto aun no ha sido tratado por el Parlamento.

9. Conclusión Final

Como antes dijera, en nuestro sistema jurídico Argentino, tenemos dos factores de atribución de responsabilidad extracontractual: la **responsabilidad subjetiva**, clásica, tradicional, y la nueva responsabilidad que está avanzando poco a poco, que es la **responsabilidad objetiva.**

¿Dónde debemos buscar las responsabilidades de los proveedores de servicio de Internet frente a la incorporación de contenidos ilícitos o que causan daño o a la Incorporación ilícita de contenidos ?

¿Se trata de una responsabilidad subjetiva u objetiva?

La primera es la que surge de la culpa en el daño, el que causó un daño debe

resarcirlo. Esa es la responsabilidad tradicional, que podríamos endilgarle quizás al buscador si le demostramos la culpa o la intencionalidad.

Su fundamento lo encontramos en los arts. 512 y 1109 del Código Civil que establecen fundamentalmente que *"La culpa del deudor en el cumplimiento de la obligación consiste en la omisión de aquellas diligencias que exigiere la naturaleza de la obligación, y que correspondiesen a las circunstancias de las personas, del tiempo y del lugar"*, y que *"Todo el que ejecuta un hecho, que por su culpa o negligencia ocasiona un daño a otro, está obligado a la reparación del perjuicio…"*

Por otro lado tenemos la responsabilidad objetiva –que tiene muchos defensores– que es la responsabilidad sin culpa, que se crea por otros motivos, que aparece para tener respuesta ante el daño, para que ciertos actores respondan aún sin haber cometido culpa. ¿Por qué así? Porque se ejerce una actividad riesgosa o peligrosa.

Creo que la responsabilidad objetiva no puede ser atribuida a Internet, porque no puede decirse que Internet sea una actividad riesgosa o peligrosa.

Me inclino rotundamente por la exclusión de Internet de este tipo de responsabilidad. Creo que Internet no es lo mismo que el fabricante de un arma o el propietario de una plataforma petrolera. Si creáramos una responsabilidad objetiva sobre Internet, además de equivocar en su origen, la estaríamos destruyendo. Sería la destrucción de un medio que ha beneficiado

enormemente al mundo; el acceso al conocimiento y a la información que nos ha dado Internet no puede ser desconocido.

El concepto de actividad peligrosa o riesgosa es por su naturaleza un concepto relativo y depende del estado de avance de la ciencia y de la técnica en un sector determinado; lo que lleva a calificar de peligrosas a actividades que antes no lo eran o viceversa.

Se debe tener en cuenta que la utilización de la informática en el mundo actual ha dado lugar a múltiples usos, de los cuales algunos pocos pueden implicar actividades peligrosas pero no así otros. Pareciera, y así lo ha considerado la jurisprudencia en algún caso, que la utilización de la informática en el manejo de los bancos de datos podría considerarse una actividad peligrosa [ii] , así como también el desarrollo de determinados software destinado a actividades industriales que son en si peligrosas, como podría ser el destinado a centrales nucleares, etc.

Bustamante Alsina, nos dice que los sistemas automatizados de información que emplean la informática, no son cosas peligrosas que dañen por sí mismas, sino instrumentos que el hombre maneja o acciona a su voluntad.
Reitero que se ha dicho que "*No hay cosas peligrosas o no peligrosas en sí, sino que la tal peligrosidad depende de una situación jurídica integrada por la cosa y la particular circunstancia en que se originó el daño* [ii]

Tradicionalmente se ha considerado que la responsabilidad objetiva debe estar asociada con actividades que son potencialmente peligrosas y que tienen una alta probabilidad de daño. Tal el caso de la energía eléctrica, la producción o tratamiento de explosivos o materiales radioactivos.

Se ha dicho también con acierto: *"la aplicabilidad del artículo 1113 requiere, en cualquier hipótesis, que la cosa tenga una intervención activa en la producción del daño. La caracterización de este concepto ha dado lugar a arduas discusiones doctrinarias en Francia; pero es de entender que la intervención de la cosa es activa cuando tiene acción nociva, o sea, cuando ella causa el daño; en tanto –por lo contrario- su intervención es pasiva cuando no causa el daño, el cual no nace de la cosa de que se trata"* ii.

Creo que cuando se trata de perjuicios que son causados por la cosa interviniente en forma directa , y esa cosa es un elemento de potencial peligro, podría regir el sistema de responsabilidad objetiva del artículo 1113 2º párrafo del Código Civil, pero cuando la cosa no interviene autónomamente en la producción del daño, sino respondiendo al accionar del operador, debe ser aplicado un criterio de atribución de responsabilidad subjetiva conforme al artículo 1109 del Código Civil.

¿Cuál es la naturaleza del ISP? ¿Son editores de la información?

Estimo que no, ni el que transmite técnicamente la información ni el buscador que me lleva a ella editaron la información. Ellos no crean el link, se crea

automáticamente con la indexación que realiza el algoritmo creado. Son sólo distribuidores de información, reitero, no le podemos atribuir entonces una responsabilidad objetiva. Pero sí una responsabilidad subjetiva, en la medida que le podamos probar que ellos conocían el hecho, que fueron partícipes, que tuvieron culpa, que hubo negligencia de su parte.

Sentado este criterio de atribución de responsabilidad subjetiva, debemos ver ahora en que casos se da la misma.

En primer término considero que los ISP son plenamente responsables con relación a los contenidos propios, generándose en ese supuesto su plena responsabilidad objetiva, tanto por transmitir como por alojar estos contenidos que le pertenecen.

Pero con relación a los contenidos que le son ajenos y que son fundamentalmente los que transmite o aloja, creo que cualquiera sea la postura adoptada, éste tipo de proveedores sólo podría tener una responsabilidad subjetiva, que surgiría de su negligencia manifiesta.

También sería responsable cuando se le comunicó la existencia de un contenido ilícito y no tomó las medidas necesarias para evitar que el ilícito se continúe cometiendo.

Podemos afirmar que coincidimos con el consenso doctrinario hoy en día existente en cuanto que sólo cabe hacer responsable a los ISP incluyendo dentro de ellos a los buscadores en dos situaciones:

- Cuando la incorporación ilícita del contenido es manifiesta y no pudo ser ignorada por el proveedor;

- Cuando la incorporación ilícita del contenido no es manifiesta, pero el proveedor ha sido notificado de la existencia de esos contenidos y no toma de inmediato las medidas necesarias para retirar dicho contenido.

Fuera de estos casos creo que no existe responsabilidad de los ISP ya que razones tecnológicas generalmente les impiden ejercer un control permanente de los contenidos de terceros que transmiten o alojan, como también porque aceptar su responsabilidad y consecuentemente para evitarla obligarlos a eliminar o bloquear contenidos que cree ilícitos, implicaría ni mas ni menos que legalizar la privatización de la censura, toda vez que los ISP, fuera de los casos de contenidos manifiestamente ilícitos, serían quienes disciernen si un contenido es lícito o ilícito, si es nocivo o no.

_____

Buenos Aires, Agosto de 2014

Aspectos civiles y administrativos de las redes sociales. Libertad de expresión en las redes sociales

Horacio Gutiérrez Gutiérrez. Agosto 2014

Ponencia FIADI 2014. Aspectos civiles y administrativos de las redes sociales. Libertad de expresión en las redes sociales.

2 Horacio Gutiérrez Gutiérrez

Contenido

Ponencia FIADI 2014. Aspectos civiles y administrativos de las redes sociales. Libertad de expresión en las redes sociales.

Horacio Gutiérrez Gutiérrez

IResumen.

Se repasa la influencia de las redes sociales como fenómeno de comunicación e interacción entre personas, su capacidad de multiplicar la difusión de ideas, imágenes y noticias y como su abuso configurado como libertad de expresión, puede afectar los derechos de terceras personas. Conceptos clave: Libertad de expresión, redes sociales, privacidad, transparencia, divulgación no autorizada.

II. Libertad de expresión.

La manifestación del derecho a la libertad de expresión corresponde en primera instancia a la raíz etimológica exprimere, que tiene el sentido originario de movimiento del interior hacia el exterior, presión hacia fuera. Sin embargo el término tiene diversos sentidos dependiendo de las diferentes

disciplinas como se describe a continuación: • En Estética se entiende como la propiedad que posee una obra de arte para suscitar emociones, sentimientos. • En Lingüística es la palabra o grupo de palabras utilizadas para manifestar sentimientos, pensamientos, opiniones y también es el significante, lo que es dicho, esto es, el enunciado •

En Algebra es el conjunto de términos que representan una cantidad • En Psicología es el comportamiento exterior, espontáneo o intencional, que traduce emociones o sentimientos; por ejemplo: la expresión de alegría; la expresión de sorpresa.

Por otra parte, el significado de libertad de expresión contenido en el diccionario de la Real Academia de la Lengua Española se refiere como el derecho de manifestar, defender y propagar las opiniones propias, esta definición resulta básica para plantear el alcance de este derecho y las posibles limitaciones en su ejercicio primordialmente cuando se expresa en las redes sociales. La libertad de expresión forma parte del conjunto de derechos fundamentales reconocidos en las primeras declaraciones de derechos revolucionarias del siglo XVIII, y tiene su fundamento y es manifestación externa de otro derecho fundamental: la libertad ideológica.

Más aún la libertad de expresión es un derecho de defensa o derecho de libertad, un tipo de derecho subjetivo en el que la posición jurídica que se define es una posición de libertad: el titular tiene la posibilidad de hacer o no hacer lo permitido Reconociendo que es una característica de las personas la

libre voluntad acompañada del libre pensamiento, se identifican las redes sociales como vehículo para la difusión ilimitada e indiscriminada de ideas, expresiones y propagación de opiniones. Este argumento está soportado por el artículo 13 de la Convención Americana sobre Derechos Humanos que señala que la libertad de pensamiento y expresión "comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole..." términos que establecen literalmente que quienes están bajo la protección de la Convención tienen no sólo el derecho y la libertad de expresar su propio pensamiento, sino también el derecho y la libertad de buscar, recibir y difundir informaciones e ideas de toda índole.

En el artículo 13 se distinguen dos dimensiones de la libertad de expresión, primero que nadie sea arbitrariamente impedido de manifestar su propio pensamiento y representa, por tanto, un derecho de cada individuo; segundo, implica un derecho colectivo a recibir cualquier información y a conocer la expresión del pensamiento ajeno. Asumiendo el concepto de mercado de ideas1 planteado por los juristas estadounidenses Wendell y Brandeis, cuando se tienen condiciones de igualdad en la manifestación de ideas (libertad de expresión), será posible que los individuos puedan apreciar cuáles de ellas son verdaderas, falsas, o relativas. Este argumento es clave en la sociedad de la información y por supuesto en las redes sociales, donde se abre la posibilidad de que todo individuo pueda expresar libremente sus ideas y con una estrategia adecuada de difusión (blogs, twitter, etc) posicionarse como un agente de influencia en el “mercado” global de pensadores. El derecho a la libertad de expresión en formas políticas se extiende al discurso simbólico o

conducta expresiva, como la quema de banderas, las colecciones de firmas para exigir la renuncia de los miembros del gobierno, la distribución de folletos y la exhibición de pancartas. Retomando la característica del derecho a la libertad de expresión de no discriminar entre información e ideas consideradas como útiles o correctas, sin estar limitada a expresiones políticas, culturales o artísticas por lo que también puede incluir expresiones controversiales, falsas, difamatorias o incluso haciendo mofa a otras personas, que es donde surge el verdadero problema del uso y abuso de las redes sociales.

1 PINAIRE, Brian K. Marketplace of Ideas Theory. American Civil Liberties. United States of America, 2012 [En Línea] <http://uscivilliberties.org/themes/4099-marketplace-of-ideas-theory.html > [Consulta 05.06.14]

III. El papel de las redes sociales.

En esta ponencia se busca establecer un marco de referencia de los límites a la libertad de expresión en las redes sociales, basado en las consideraciones anteriores, resaltando la pertinencia del uso responsable de la tecnología de información. La base del análisis es el establecimiento de un marco de referencia que de respuesta a las preguntas siguientes del ejercicio de la libertad de expresión:

• ¿Es esta libertad susceptible de ser limitada de alguna manera? • ¿Es correcto establecer un sesgo a un derecho que en principio pareciera ser

absoluto? • Y más importante aún si es esto posible ¿Quién debe establecer este límite y en dónde?

Para ilustrar la dimensión del impacto de las redes sociales me baso en la historia de Robin Hood con la que muchas personas están familiarizados, el forajido que tomaba los bienes de los ricos para entregarlos a los pobres y habitaba en las profundidades del bosque de Sherwood mientras eludía la acción de la justicia, encabezada por el sheriff de Notingham, aprovechando que la densidad del refugio dificultaba su localización y captura. Este relato es un reflejo de la condición humana que tiende a buscar opciones para lograr una igualdad entre las diferentes clases sociales, ya sea tomando lo que pertenece al rico, mediante impuestos confiscatorios o como lo planteo en esta ponencia tomando el bien más preciado, el honor con apoyo de la tecnología y las redes sociales.

Como fenómeno de divulgación y vinculación entre personas, las redes sociales se han convertido en el medio ideal para la difusión de imágenes y videos en los que se exhiben personas en diferentes situaciones, algunas de ellas que pueden considerarse en el límite de la afectación a la privacidad. Otra práctica común es el uso de las redes sociales como plataforma para la denuncia masiva de acciones y prácticas corruptas de servidores públicos, que en algunos casos han resultado efectivos en términos mediáticos de renuncia o remoción de funcionarios, pero al ser imágenes obtenidas sin autorización de las personas pueden infringir sus derechos y constituirse en una falta que puede ser merecedora de una sanción. Por último me refiero al tratamiento

que se realiza en fotografías de personas famosas para agregar texto o modificarlas y difundirlas, lo que se conoce como memes. El paralelismo entre Robin Hood y los usuarios de las redes sociales es el marco para describir la problemática del uso indiscriminado de las redes sociales: 1. Privacidad e intimidad, 2. Afectación intencional de terceros empleando medios electrónicos. 3. Libertad de expresión.

IV. El reto de la libertad de expresión en las redes sociales.

El derecho a difundir información e ideas es el aspecto más obvio de la libertad de expresión, que permite decirle a otros lo que uno piensa o conoce, de manera privada o usando los medios. Pero la libertad de expresión tiene un propósito más grande ya que le permite a toda persona acceder a un espectro de información y puntos de vista tan amplio como sea posible.

En la práctica la libertad de expresión, no implica que únicamente se garantice la posibilidad de que el individuo exprese sus ideas de manera libre, sino además, se debe garantizar que el resto de la comunidad virtual con quien convive en las redes sociales tenga la oportunidad de conocerlas y evaluarlas, sin menoscabo de los derechos de terceras personas. Como medio de desarrollo personal la libertad de expresión es relevante para la dignidad y la realización individual pues permite: • Obtener y compartir conocimiento, al intercambiar ideas e información libremente con los demás. Esto los hace más capaces de planificar sus vidas y de trabajar. • Cuando el estado respeta el ejercicio de la libertad de expresión, reditúa un sentimiento de seguridad y

respeto, ya que las personas se sienten más confiadas en expresar sus ideas sin temor a represalias. • Se fomenta el intercambio de opiniones informadas y la participación en un debates abierto de cualquier tema. En el caso específico de las redes sociales se han convertido en el refugio ideal para que las personas expresen sus opiniones de manera inmediata, pero también con el beneficio o riesgo de que estas se propaguen exponencialmente, las más de las veces sin control de quien la emite. Al sentirse protegidas por el anonimato las personas se sienten más seguras de expresar sus pensamientos, ideas y posiciones ideológicas, la cara negativa en muchos casos está representada por insultos o levantar falsedades en contra de terceros que pueden repercutir en la honorabilidad y reputación de estos. En este escenario nos enfrentamos con las limitaciones y excepciones a la libertad de expresión.

V. Regulación en redes sociales.

La consideración de partida es que ningún derecho o libertad tiene un carácter absoluto en cuanto a su ejercicio, esta máxima implica que el goce de ese derecho o libertad no implica afectar a terceros, por lo tanto quienes manifiesten sus opiniones deben cumplir con esa consigna ética dentro del marco del respeto y la buena fe hacia los demás. De acuerdo con Del Río2 Internet, en este caso las redes sociales, puede convertirse en una herramienta de empoderamiento para todas las personas y los pueblos del mundo sin embargo tal circunstancia requiere del reconocimiento, protección y respeto de siete derechos: 1) Acceso a Internet para todos; 2) Libertad de expresión y asociación; 3) Acceso al conocimiento; 4) Intercambio de aprendizaje y

creación - software libre y desarrollo tecnológico; 5) Privacidad, vigilancia y encriptación; 6) Gobernanza de Internet y 7) Conciencia, protección y realización de los derechos. Desde esta perspectiva, el acceso a la información y a la comunicación resulta crucial para una participación activa de la ciudadanía y de sus expresiones organizadas (red/comunicación), condición indispensable a su vez para el ejercicio de los derechos humanos. Como expresión de ideas la Libertad de Expresión también implica responsabilidad de las personas para el ejercicio razonado de este

2 DEL RÍO Sánchez, Olga. TIC, derechos Humanos y desarrollo: Nuevos Escenarios de la Comunicación Social. Universidad Autónoma de Barcelona. Barcelona, España. 2009 [En línea] <http://www.academia.edu/2441848/TIC_derechos_humanos_y_desarrollo_nuevos_escenarios_de_la_comunicacion_social_ICT_Human_Rights_and_Development_New_Subjects_of_Social_Communication>

derecho, por ello se retoman los límites que establece la Convención Americana sobre los Derechos Humanos en su artículo 13:

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a) el respeto a los derechos o a la reputación de los demás, o
b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

3. No se puede restringir el derecho de expresión por vías a medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones. Como se ha discutido la primera impresión del ejercicio del derecho a la libertad de expresión es que no debe restringirse de ninguna manera ya que es una libertad necesaria para garantizar otros derechos humanos. Por otra parte, este derecho debe ser ejercido en un marco de responsabilidad, pues los pensamientos deben poseer también claridad sobre las eventuales consecuencias que, por afectación a la moral, el orden público o a terceros, se puedan generar. No obstante lo anterior y retomando el caso de las redes sociales, la recepción y difusión de informaciones e ideas de manera indiscriminada, puede incluir expresiones que pocas sociedades pueden tolerar, tal como la incitación al asesinato o la venta de pornografía a los niños. Por los tanto, la libertad de expresión no es absoluta y puede ser limitada cuando entra en conflicto con otros derechos.

Teniendo en cuenta que el balance entre libertad de expresión y censura resulta complejo, y que el conflicto se presenta con frecuencia por los malentendidos acerca del alcance de lo que se pretende proteger, es

importante comprender las implicaciones del Derecho a la Libertad de Expresión, establecido por la Corte Interamericana de Derechos Humanos ubicándolo como un derecho no absoluto y que puede, en consecuencia, ser objeto de restricciones, sin embargo, las restricciones a la libertad de expresión deben ser proporcionales y resultado de la sus posibles alcances, como son: • ¿La libertad de expresión abre el espacio para afectar los derechos de terceros? • ¿La libertad de expresión puede atentar contra la moral o la seguridad nacional? Por esta situación se deben resaltar los principios que permitan dilucidar entre libertad de expresión y censura; donde la claridad en el derecho, la materia política y la práctica es esencial para ponderar sus posibles colisiones con otros derechos. El derecho internacional sostiene que la libertad de expresión debe ser la regla. Las limitaciones son la excepción, solamente permitidas para proteger: • Los derechos o reputaciones de los demás • La seguridad nacional • El orden público • La salud pública • La moral La excepción a la Libertad de Expresión se establece el artículo 13 de la Convención Americana sobre

Derechos Humanos en su párrafo quinto:

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional. Es importante establecer que los preceptos legales que limiten el derecho de expresión, deberán ser claros y contener los siguientes elementos: a) Los gobernados, en este caso los usuarios de las redes sociales,

deberán tener una oportunidad razonable de saber lo que está prohibido, de manera de poder actuar en consecuencia. b) Las decisiones para este ensayo las publicaciones de los internautas, que afecten los derechos humanos deben ser realizadas por organismos que representen la voluntad popular. c) Debe existir un fin legítimo para restringir la libertad de expresión, la lista de fines legítimos no puede ser ampliada. d) Las restricciones a la libertad de expresión deben ser realmente necesaria. Incluso si una restricción está prevista por una ley clara y persigue un fin legítimo, solamente superará la prueba si es verdaderamente necesaria para la protección del fin legítimo.

VI. Conclusiones.

La libertad de información es una extensión de la libertad de expresión, éste último es un derecho humano fundamental que se encuentra reconocido por diversos instrumentos internacionales, este derecho no solo comprende el contenido sino también los medios de expresión utilizados, dicho de otro modo todos tienen derecho a la libertad de expresión y ésta incluye el derecho a buscar, difundir y recibir información.

Su origen se encuentra en el pensamiento liberal, en movimientos sociales como la Revolución Francesa o la Independencia de los Estados Unidos. Válidamente podemos señalar que la libertad de expresión implica cargas y obligaciones que un principio eran de no hacer a obligaciones de hacer, consistiendo una serie de cargas positivas para permitir la difusión, recepción, investigación de la información por parte de los ciudadanos incluyendo la

propia información del estado para los ciudadanos. Diversas formas que han existido a lo largo del tiempo para que los seres humanos se expresen sufren actualmente renovaciones que en vez de aniquilarlas las fortalece, tal es el caso de la Fotografía Digital la cual con la ayuda de las redes sociales ha desarrollado un nuevo tipo de periodismo y es el llamado periodismo ciudadano. Puede ejercerse a través de cualquier medio, desde el clásico escrito, medios de comunicación masiva, prensa radio, televisión, cinematografía, llegando hasta las contemporáneas tecnologías de la información y comunicación y tienen su mayor exponente en las redes sociales. Las nuevas tecnologías de información y comunicación ofrecen nuevos medios por medio de los cuales los individuos pueden manifestar sus ideas, emociones, opiniones sin embargo es necesario e indispensable que se cuente con un Marco Legal que garantice el libre acceso a estos nuevos medios y más aún que no haya restricciones en su uso, con excepción de las que los límites y excepciones imponen.