FACULTAD DE DERECHO Y CIENCIA POLITICA

Escuela Profesional de Derecho

TESIS

ANÁLISIS DE LAS APLICACIONES DE INTERNET QUE VULNERAN EL DERECHO FUNDAMENTAL A LA INTIMIDAD DE SUS USUARIOS EN EL DISTRITO DE PAUCARPATA, AREQUIPA 2014 – 2015

PRESENTADO POR:

Macedonio Enrique Santa Cruz Aco

ASESORES:

Luis Jordán Parra

Víctor Augusto Benjamín Pantigoso Bustamante

PARA OPTAR AL TÍTULO PROFESIONAL DE ABOGADO

Arequipa- Perú

2016

UAP UNIVERSIDAD ALAS PERUANAS

Facultad de Derecho y Ciencias Políticas
Escuela Profesional de Derecho

DICTAMEN DE ASESORIA DE TESIS

Arequipa, 18 de enero del 2016

Que presenta a la Directora de la Escuela Académica Profesional de Derecho y Ciencias Políticas Gigliola Arias Huiza, el catedrático asesor Dr. Luis Jordán Parra, del trabajo de Tesis titulado, "***ANÁLISIS DE LAS APLICACIONES DE INTERNET QUE VULNERAN EL DERECHO FUNDAMENTAL A LA INTIMIDAD DE SUS USUARIOS EN EL DISTRITO DE PAUCARPATA, AREQUIPA 2014 – 2015***" Presentado por el bachiller en Derecho Macedonio Enrique Santa Cruz Aco, para optar el Título Profesional de ABOGADO.

Señora Directora:

Cumplo con comunicar a usted, que el Bachiller en mención, ha terminado el desarrollo del trabajo de Tesis, habiendo cumplido con las exigencias del Reglamento de Grados, para ser presentada al Jurado, manteniendo un orden expositivo, precisando los aspectos normativos, doctrinales y metodológicos, que habilita para aspirar al Título Profesional de abogado.

El proceso del desarrollo de la Tesis presenta los aspectos siguientes:

El problema de investigación: *versa sobre* "***las aplicaciones de internet que vulneran el derecho fundamental a la Intimidad de sus usuarios"***, el cual se basa en primer orden en el Art.2 Inc. 6 de nuestra Constitución Política del Perú, el cual prescribe "***A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar***. Del mismo modo en el Art. 2 Inc. 7 del mismo cuerpo legal que establece "***Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias***"; siguiendo con la línea de ideas, disgregamos como el derecho a la intimidad, ***aquel en el que se encuentran un núcleo de personas al que regularmente queremos proteger con un ánimo mucho mayor, por considerarlo inseparable de la esencia misma de nuestra propia vida y de la privacidad***" por otro lado, cabe señalar la ley de reciente implementación conocida

como Ley de Protección de Datos Personales que nace en función al Inc. 6 del Art. 2 de la Constitución para el ámbito digital, dispone "***La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen***." Lo cual hace referencia al mencionado derecho a la intimidad en el aspecto de dato personal.

De lo establecido anteriormente la ley no señala, hasta donde son sus alcances en lo referente a la red conocida como Internet, debido a que los citados referentes legales, no concluyen en una regulación específica referida a la intimidad propiamente dicha, pues, ***no existe una correspondencia legal de lo señalado y lo que sucede en la realidad, más aún cuando no existe un sistema jurídico específico y solo normas generales de orden constitucional, en otro aspecto la ley de protección de datos personales, que garantiza el Art.2 Inc. 6 de nuestra constitución, al estar facultada para realizar una ponderación de derechos constitucionales ante un conflicto de estos, no cuenta con vínculos o acuerdos con el Tribunal Constitucional que si puede hacerlo, del mismo modo, nuestro ordenamiento no cuenta con formas de resarcir un daño al usuario vulnerado en su intimidad cuando haya aplicaciones de Internet de por medio, de ello se colige que la regulación y protección hacia el ciudadano es asistemática, aislada e inaccionable***, pues no existe un marco que corresponda a la defensa de derechos tan singulares y propios.

Desarrollando el presente problema investigativo, en la realidad, señalamos que ***cualquier actividad o consulta, que llevemos a cabo en internet, deja una huella o marca que permite nuestra identificación, esa huella personal permite la creación de perfiles online de los usuarios de Internet, los perfiles así creados permiten a los prestadores de servicios o aplicaciones de Internet, enviar la denominada "publicidad online comportamental" es en este punto, donde el usuario de internet, siendo titular de su información personal, pierde prácticamente el control sobre ella y es allí donde la intimidad de las acciones que se realizan en Internet a través de aplicaciones se ve vulnerada***, de igual forma, no debe olvidarse, que al hacer uso de estas tecnologías ***aceptamos un acuerdo, el mismo que al analizarse rigurosamente y legalmente trae consigo el empleo de términos ambiguos, haciéndose remisiones entre diferentes políticas como, por ejemplo, de la política de privacidad general a la política de cookies o viceversa, se fragmenta deliberadamente la información para evitar que el***

usuario tenga conocimiento cabal de sus derechos y obligaciones así como de los derechos y obligaciones del titular del sitio web o aplicación, es así que desde el punto de vista jurídico, una forma de intentar frenar esta asimetría, en cuanto al control de la información personal del usuario de internet, ***se encuentra en regular los puntos citados mediante un marco legal sistemático***.

El presente trabajo se circunscribió al Distrito de Paucarpata, provincia y departamento de Arequipa – Perú. Esto debido a que es uno de los distritos más populosos y grandes de la ciudad de Arequipa.

1. ***Marco Teórico:*** La teoría que presenta el trabajo de investigativo está basada, en el derecho a la intimidad disgregado en la privacidad y los datos personales, así también en que somos el país que hace mayor uso de internet de Latinoamérica, del mismo modo, la población conoce el termino Intimidad jurídicamente en relación a las aplicaciones de Internet.

2. ***Los Objetivos e Hipótesis:*** Para poder absolver el problema de investigación formulado, se ha establecido el objetivo general: ***Analizar las aplicaciones de Internet que afectan el derecho fundamental a la intimidad de sus usuarios***. Siendo la Hipótesis planteada, ***Es probable que la regulación de las aplicaciones de Internet a través de un marco normativo específico, garantice el derecho a la intimidad de los usuarios de internet***

3. ***Método de investigación:*** El presente trabajo investigativo es de corte analítico – explicativo, porque se basa en analizar cualitativamente y explicar cuantitativamente las injerencias al derecho a la intimidad que suceden cotidianamente en las aplicaciones de Internet, el **diseño de la Investigación es, *no experimental,*** debido a que se realizó ***sin manipular*** deliberadamente o intencionadamente las variables, y en la cual los sujetos son observados en su ambiente cotidiano, en su realidad, porque una vez establecido el problema de investigación, se procederá a buscar los argumentos fácticos que justifiquen el análisis de las "***Aplicaciones de internet que vulneran el derecho fundamental a la intimidad de sus***

usuarios". La población está constituida por el 44.9% de 125255 personas que en calidad de usuarios de Internet o que acceden a Internet, habitan en el distrito de Paucarpata. La muestra de la que parte el presente trabajo investigativo consta de 203 personas, es decir usuarios que usan Internet pues son los que están en constante relación con las aplicaciones de Internet y conocen las vulneraciones que se suscitan en este medio.

4. ***Resultado de la Investigación:*** En el presente trabajo de investigación se demuestra que la población no conoce formas de manejo, control y protección de su información, ni de las normas sobre las cuales sustentar su derecho a la intimidad, en consecuencia, no reconocen en sí mismos tal garantía constitucional y consideran este hecho como parte de su cotidianidad.

OPINIÓN DEL ASESOR.

Desde el punto de vista de la investigación y el análisis jurídico desarrollado; el presente trabajo investigativo reviste profuso interés para el desarrollo normativo y teórico, en el sentido de que la Intimidad es un derecho constitucional consagrado en la Constitución, de lo cual toda persona es titular, en consecuencia, el uso de aplicaciones que nos permitan navegar en Internet, impidiendo el manejo que podamos hacer de nuestra información íntima, constituye una agresión a los derechos básicos de la persona, ante lo cual nuestra normativa se encuentra carente de acción, hecho por el cual, el presente trabajo importa un real beneficio jurídico.

Por las consideraciones expuestas considero que la asesoría ha culminado con sus objetivos, pues el Bachiller ha desarrollado su Tesis a entera satisfacción, mostrando dedicación y capacidad argumentativa. Por lo tanto, la Tesis está concluida y lista para ser sustentada.

Atentamente,

Luis Jordán Parra

ABOGADO

CAA: 2481

UNIVERSIDAD ALAS PERUANAS

Facultad de Derecho y Ciencias Políticas
Escuela Profesional de Derecho

DICTAMEN DE ASESORIA DE TESIS

Arequipa, 18 de enero del 2016

Que presenta a la Directora de la Escuela Académica Profesional de Derecho y Ciencias Políticas Gigliola Arias Huiza, el catedrático asesor Mag. Víctor A. B. Pantigoso Bustamante, del trabajo de Tesis titulado, "***ANÁLISIS DE LAS APLICACIONES DE INTERNET QUE VULNERAN EL DERECHO FUNDAMENTAL A LA INTIMIDAD DE SUS USUARIOS EN EL DISTRITO DE PAUCARPATA, AREQUIPA 2014 – 2015***" Presentado por el bachiller en Derecho Macedonio Enrique Santa Cruz Aco, para optar el Título Profesional de ABOGADO.

Señora Directora:

Cumplo con comunicar a usted, que el Bachiller en mención, ha terminado el desarrollo del trabajo de Tesis, habiendo cumplido con las exigencias del Reglamento de Grados, para ser presentada al Jurado, manteniendo un orden expositivo, precisando los aspectos normativos, doctrinales y metodológicos, que habilita para aspirar al Título Profesional de abogado.

El proceso del desarrollo de la Tesis presenta los aspectos siguientes:

El problema de investigación: *versa sobre* "***las aplicaciones de internet que vulneran el derecho fundamental a la Intimidad de sus usuarios"***, el cual se basa en primer orden en el Art.2 Inc. 6 de nuestra Constitución Política del Perú, el cual prescribe "***A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar***. Del mismo modo en el Art. 2 Inc. 7 del mismo cuerpo legal que establece "***Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias***"; siguiendo con la línea de ideas, disgregamos como el derecho a la intimidad, ***aquel en el que se encuentran un núcleo de personas al que regularmente queremos proteger con un ánimo mucho mayor, por considerarlo inseparable de la esencia misma de nuestra propia vida y de la privacidad***" por otro lado, cabe señalar la ley de reciente implementación conocida

como Ley de Protección de Datos Personales que nace en función al Inc. 6 del Art. 2 de la Constitución para el ámbito digital, dispone "***La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen***." Lo cual hace referencia al mencionado derecho a la intimidad en el aspecto de dato personal.

De lo establecido anteriormente la ley no señala, hasta donde son sus alcances en lo referente a la red conocida como Internet, debido a que los citados referentes legales, no concluyen en una regulación específica referida a la intimidad propiamente dicha, pues, ***no existe una correspondencia legal de lo señalado y lo que sucede en la realidad, más aún cuando no existe un sistema jurídico específico y solo normas generales de orden constitucional, en otro aspecto la ley de protección de datos personales, que garantiza el Art.2 Inc. 6 de nuestra constitución, al estar facultada para realizar una ponderación de derechos constitucionales ante un conflicto de estos, no cuenta con vínculos o acuerdos con el Tribunal Constitucional que si puede hacerlo, del mismo modo, nuestro ordenamiento no cuenta con formas de resarcir un daño al usuario vulnerado en su intimidad cuando haya aplicaciones de Internet de por medio, de ello se colige que la regulación y protección hacia el ciudadano es asistemática, aislada e inaccionable***, pues no existe un marco que corresponda a la defensa de derechos tan singulares y propios.

Desarrollando el presente problema investigativo, en la realidad, señalamos que ***cualquier actividad o consulta, que llevemos a cabo en internet, deja una huella o marca que permite nuestra identificación, esa huella personal permite la creación de perfiles online de los usuarios de Internet, los perfiles así creados permiten a los prestadores de servicios o aplicaciones de Internet, enviar la denominada "publicidad online comportamental" es en este punto, donde el usuario de internet, siendo titular de su información personal, pierde prácticamente el control sobre ella y es allí donde la intimidad de las acciones que se realizan en Internet a través de aplicaciones se ve vulnerada***, de igual forma, no debe olvidarse, que al hacer uso de estas tecnologías ***aceptamos un acuerdo, el mismo que al analizarse rigurosamente y legalmente trae consigo el empleo de términos ambiguos, haciéndose remisiones entre diferentes políticas como, por ejemplo, de la política de privacidad general a la política de cookies o viceversa, se fragmenta deliberadamente la información para evitar que el***

usuario tenga conocimiento cabal de sus derechos y obligaciones así como de los derechos y obligaciones del titular del sitio web o aplicación, es así que desde el punto de vista jurídico, una forma de intentar frenar esta asimetría, en cuanto al control de la información personal del usuario de internet, ***se encuentra en regular los puntos citados mediante un marco legal sistemático***.

El presente trabajo se circunscribió al Distrito de Paucarpata, provincia y departamento de Arequipa – Perú. Esto debido a que es uno de los distritos más populosos y grandes de la ciudad de Arequipa.

1. ***Marco Teórico:*** La teoría que presenta el trabajo de investigativo está basada, en el derecho a la intimidad disgregado en la privacidad y los datos personales, así también en que somos el país que hace mayor uso de internet de Latinoamérica, del mismo modo, la población conoce el termino Intimidad jurídicamente en relación a las aplicaciones de Internet.

2. ***Los Objetivos e Hipótesis:*** Para poder absolver el problema de investigación formulado, se ha establecido el objetivo general: ***Analizar las aplicaciones de Internet que afectan el derecho fundamental a la intimidad de sus usuarios***. Siendo la Hipótesis planteada, ***Es probable que la regulación de las aplicaciones de Internet a través de un marco normativo específico, garantice el derecho a la intimidad de los usuarios de internet***

3. ***Método de investigación:*** El presente trabajo investigativo es de corte analítico – explicativo, porque se basa en analizar cualitativamente y explicar cuantitativamente las injerencias al derecho a la intimidad que suceden cotidianamente en las aplicaciones de Internet, el **diseño de la Investigación es, *no experimental,*** debido a que se realizó ***sin manipular*** deliberadamente o intencionadamente las variables, y en la cual los sujetos son observados en su ambiente cotidiano, en su realidad, porque una vez establecido el problema de investigación, se procederá a buscar los argumentos fácticos que justifiquen el análisis de las "***Aplicaciones de internet que vulneran el derecho fundamental a la intimidad de sus***

usuarios". La población está constituida por el 44.9% de 125255 personas que en calidad de usuarios de Internet o que acceden a Internet, habitan en el distrito de Paucarpata. La muestra de la que parte el presente trabajo investigativo consta de 203 personas, es decir usuarios que usan Internet pues son los que están en constante relación con las aplicaciones de Internet y conocen las vulneraciones que se suscitan en este medio.

4. ***Resultado de la Investigación:*** En el presente trabajo de investigación se demuestra que la población no conoce formas de manejo, control y protección de su información, ni de las normas sobre las cuales sustentar su derecho a la intimidad, en consecuencia, no reconocen en sí mismos tal garantía constitucional y consideran este hecho como parte de su cotidianidad.

OPINIÓN DEL ASESOR.

Desde el punto de vista de la investigación y el análisis jurídico desarrollado; el presente trabajo investigativo reviste profuso interés para el desarrollo normativo y teórico, en el sentido de que la Intimidad es un derecho constitucional consagrado en la Constitución, de lo cual toda persona es titular, en consecuencia, el uso de aplicaciones que nos permitan navegar en Internet, impidiendo el manejo que podamos hacer de nuestra información íntima, constituye una agresión a los derechos básicos de la persona, ante lo cual nuestra normativa se encuentra carente de acción, hecho por el cual, el presente trabajo importa un real beneficio jurídico.

Por las consideraciones expuestas considero que la asesoría ha culminado con sus objetivos, pues el Bachiller ha desarrollado su Tesis a entera satisfacción, mostrando dedicación y capacidad argumentativa. Por lo tanto, la Tesis está concluida y lista para ser sustentada.

Atentamente,

Mag. Víctor A.B. Pantigoso Bustamante
Docente Asesor
CAA Nº 4012

DEDICATORIA

A mis Taitas por el esfuerzo de darme la vida, su ánimo incondicional y el sosiego en los umbríos pasos de este trabajo.

A Mylalefineh y Adadi por ser mi asidero, darme su tiempo, entereza, generosidad y ser los más grandes asesores de esta existencia.

A los jueces y asesores que me prestaron su paciente crítica en la elaboración, redacción, sugerencias y precisas reflexiones.

A Bebeluz, Rempicka y Litha por regalarme dulces dingolondangos.

A Selene por su gran consejo y apoyo.

Al Dios de los datos digitales y sus arcángeles Copy y Paste

Al complejo mundo que me ha tocado conocer…

AGRADECIMIENTO

A mis maestros y asesores, solidarios conductores en la concreción de este trabajo.

RESUMEN

Este trabajo investigativo tiene como objeto desarrollar el derecho a la intimidad en relación a las diversas aplicaciones de Internet, analizando como referente, supuestos de vulneración que se suscitan sobre los derechos del usuario que hace uso de diversas aplicaciones de Internet, realizando un estudio exhaustivo de corte cualicuantitativo cuyo método es analítico - explicativo, realizado sobre una muestra de 203 personas con una encuesta de instrumento por un lado y un análisis hermenéutico documental por otro, sobre las políticas de privacidad de las principales aplicaciones de Internet, pronunciando como resultado de una parte, que las aplicaciones que analizan la información íntima del usuario vulneran su derecho a la intimidad, del mismo modo se pudo establecer que las aplicaciones de Internet deben de respetar la normativa nacional pidiendo que se implemente el derecho al olvido como garantía a su derecho a la intimidad, de otra parte se estableció que gran parte de las políticas de privacidad de las aplicaciones de Internet más representativas, por sus cambiantes políticas de privacidad y su ambigüedad, no brindan un real sustento al derecho a la Intimidad de los usuarios.

ABSTRACT

This investigative work has as aim to develop the right to privacy in relation to the various applications of Internet, analyzing as reference, assumptions of infringement that arise on the rights of the user who makes use of various Internet applications, undertaking an in-depth study of court qualitative quantitative is whose method analytical - explanatory, carried out on a sample of 203 people with a survey instrument by one side and a hermeneutic analysis documentary on the other, on the privacy policies of the main applications of the Internet, pronouncing as a result, a part that the applications that analyze the intimate information of the User violate their right to privacy, in the same way it was possible to establish that the applications of the Internet must To respect the national legislation calling for you to deploy the right to oblivion as a guarantee of their right to privacy, on the other hand it was established that a large part of the privacy policies of the Internet applications more representative, by changing their privacy policies and its ambiguity, do not provide a real support to the right to privacy of the users.

INTRODUCCIÓN

El tiempo, es un factor que determina los alcances informativos a los que nuestra raza tiene acceso en cada intervalo generacional, es así, que los últimos de ellos, se han visto fundamentalmente influenciados y beneficiados por la forma en la que ha evolucionado la comunicación, de tal manera que de entre los diferentes medios que la permiten, Internet ha pasado a tomar un aspecto preponderante y casi sustancial de la cultura y el desarrollo humano, abarcando desde nuestro medio de comunicación favorito, hasta un indispensable soporte educativo, socialmente ha revolucionado la perspectiva cultural del derecho, pasando de ser un servicio de comunicación social, hasta un reciente modelo económico de negocio que ha demostrado tener un potencial económico mayor, a cualquier actividad vista hasta nuestros tiempos y con miras a crecer, es así, que Internet como concepto comunicativo de interés social, pasó a verse como un modelo de negocio que se ha ido amoldando a los intereses de quienes más poder tienen, esa es la actual coalición de ideas respecto a este singular medio, sin embargo, la persona o usuario como principal actor en el desarrollo de esta red poco ha visto mejorado su estatus, muy por el contrario, el respeto y su tratativa han sufrido un menoscabo tan grande que hoy sin exagerar el termino, "hemos sido convertidos en información despersonificada" que navega en un especie de realidad paralela conocida como Internet, donde jurídicamente la persona se ha separado de sus derechos, de tal modo, que esta realidad enseña la primacía de los intereses personales sobre el bien común, afectando no solo a cada nación sino al género humano, vulnerando la libertad, dignidad, y nuestros derechos personalísimos, pasando este de ser un adjetivo social a una idea conceptual, esta idea es la que da nacimiento al presente trabajo investigativo, pretendiendo explicar las ideas antes expuestas en el presente trabajo.

La idea de Internet libre y abierta obedece a su origen y vertiginoso crecimiento, pues creaba un espacio donde se rompían las barreras étnicas, culturales, jurídicas y territoriales, donde la idea de espacio tiempo, se relativizaban, esto resultó muy atractivo a las masas cada vez más crecientes

que hacían uso de esta red, sin embargo, hoy se observa un uso cada vez más perverso de las nuevas tecnologías en menoscabo de la persona y sus derechos en Internet, es allí donde surgen hechos que colisionan con uno o algunos derechos fundamentales que proclama nuestra constitución y sus congéneres de otras naciones, pero, cuanto de lo garantizado, puede efectivizarse en un medio tan necesario e inseguro como es Internet, en caso de violarse alguno de ellos, se habrá alterado la naturaleza privada del servicio para dar lugar a un fenómeno social de importancia general que merezca una respuesta legislativa para estos tiempos y los venideros, ello constituye un real perjuicio y detrimento a nuestros derechos, así, como un hecho común a toda la población, principalmente a la más joven que es la que hace un uso más intensivo de este medio y que no sabe, ni puede ejercer debidamente sus derechos *¿porque no obligar a un servicio que se ofrece en Internet a respetar mínimamente nuestros derechos como personas entre ellos nuestra intimidad, sin menoscabar sus intereses*?

Dentro de los parámetros que dirigirán el presente trabajo investigativo se tiene por objetivo principal, "*analizar las aplicaciones de Internet que afectan el derecho fundamental a la intimidad de sus usuarios"*, del mismo modo este objetivo principal se disgrega en tres objetivos secundarios, de los cuales en primer lugar tenemos: "*identificar el manejo que las aplicaciones de Internet dan la intimidad de sus usuarios*", en segundo lugar, "*describir las formas de vulneración a la intimidad en las aplicaciones de Internet*", por último y en tercer lugar se busca, "*determinar las formas de protección a la intimidad de los usuarios en Internet*", todo lo anterior está dirigido a probar la hipótesis que discurre "*es probable que la regulación de las aplicaciones de Internet a través de un marco normativo específico, garantice el derecho a la intimidad de los usuarios de Internet*", continuando con el orden de ideas y ampliando en la estructura del presente trabajo, se optó por el diseño de investigación analítico – explicativo, pues analizará y explicará las injerencias de las aplicaciones de Internet respecto al derecho a la intimidad de sus usuarios, por otro lado el presente trabajo investigativo es corte holista, es decir exhaustivo, sistémico o panorámico, así mismo, la presente investigación, por el tenor de su contenido es de carácter reciente o actual, se ubica principalmente dentro del derecho

informático y constitucional con algunos atisbos del derecho internacional privado, civil y penal, es de naturaleza teórica, pues confluyen diversos constructos teóricos, que serán contrastados con la realidad, buscando sustentar o explicar las causas o efectos, de la relación del usuario de Internet con las aplicaciones de Internet; el enfoque elegido para el presente trabajo investigativo es cualicuantitativo, cuyo método en primer orden será el de análisis e interpretación documental (hermenéutico), así como, el método investigativo explicativo; la técnica elegida para el presente trabajo de investigación será de dos etapas, en primer lugar la de acopio y análisis documental y en segundo lugar será la encuesta, la cual corresponderá al trabajo de campo.

El presente trabajo de investigación se estructura en capítulos, de los cuales el primero, corresponde al planteamiento metodológico, el cual describirá la realidad problemática, delimitando el problema de investigación, buscando responder la interrogante *¿por qué las aplicaciones de internet afectan el derecho fundamental a la Intimidad de sus usuarios en el distrito de Paucarpata, Arequipa 2014 – 2015*?; el capítulo segundo se encargará del desarrollo del marco teórico, cuyo contenido son los antecedentes de la investigación, las bases teóricas que contienen algunas teorías que serán de especial aporte al derecho, las diversas bases legales que se relacionan al vacío jurídico presentado, así como la definición y desarrollo de los principales términos básicos en relación al tema; en el tercer capítulo, se plantea y detalla la hipótesis con sus respectivas variables, que serán operacionalizadas o disgregadas en sus respectivos factores o dimensiones así como sus respectivos indicadores; el capítulo cuatro delinea la metodología de la investigación desplegando el diseño, el tipo y nivel de la investigación, el enfoque, método la población y muestra elegida para el presente trabajo investigativo, así mismo, presenta las técnicas, instrumentos y los criterios de validación y confiabilidad del instrumento; en el quinto capítulo se realiza el análisis e interpretación de los resultados obtenidos luego de la aplicación del instrumento, presentando las respectivas tablas de tabulación con sus gráficos, seguido a ello deviene la prueba de la hipótesis que resulta positiva para el presente y la discusión de los resultados en relación a los datos obtenidos, las

variables medidas, su concordancia con la hipótesis y los constructos teóricos presentados; por último en el capítulo sexto, se presentan las conclusiones y recomendaciones a las que se ha llegado luego de consumar el proceso investigativo e interpretar los resultados.

CONTENIDO

CAPÍTULO I
PLANTEAMIENTO METODOLÓGICO

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

El fundamento del problema radica en la contradicción de lo establecido en la Constitución como garantía fundamental y los derechos que deberían proyectarse y protegerse mínimamente en las aplicaciones de Internet, en consecuencia, **no existe una correspondencia legal de lo señalado y lo que sucede en la realidad, más aún cuando no existe una normativa específica y solo normas generales de orden constitucional u orientadas a proteger situaciones referentes a Internet y su acceso**, de ello para agravar la problemática no existe un ente regulador o garante de los derechos íntimos de la persona en el ciber espacio o la megared conocida como Internet, que como todos sabemos es un medio de uso masivo, rápido, cuyo costo de uso es muy pequeño y comunicativamente es versátil, debido a que desde nuestro hogar hasta en nuestro celular, podemos acceder a esta red donde se interrelacionan, desde estados, empresas, hasta el desprotegido ciudadano.

De lo anterior uno de los más apremiantes fenómenos jurídicos a los que está teniendo que enfrentarse nuestra sociedad, estado y legislación es la generalización del uso de Internet como instrumento de

comunicación y comercio especialmente entre otros usos, **por lo tanto es imperativo definir en el más juicioso detalle sistemas jurídicos que garanticen a un costo mínimo o razonable, la protección de los derechos fundamentales, principalmente los referidos a la protección de la Intimidad, privacidad y de los datos personales que de esta se pueden generar**, de ello **debe ponerse especial énfasis tanto sobre la protección y el ejercicio que se pueda hacer de los derechos sustanciales, en los casos de violación a los mismos**, **de otro lado resaltar los vacíos y deficiencias que derivan de la carencia de normativa que pueda aplicarse a las actividades informáticas y de uso común dentro de la red conocida como Internet (esfera virtual)**.

En el plano nacional y local, es un hecho señalar que nuestra juventud principalmente la más joven hace uso de Internet en sus hábitos comunicativos y de otra índole más que cualquier otra persona de otras edades, tal es así que Abel Revoredo en su artículo "Adolescentes y Redes Sociales", hace mención a la situación de desprotección en la que se encuentran nuestros jóvenes ciudadanos, ***pues somos los que mayor tiempo usamos Internet en el mundo para participar en una red social***, es así, que el autor realiza una crítica a nuestra flamante y recién entrada en plena vigencia ley de protección de datos personales, **(Revoredo, 2013)** "*Si bien nuestra norma de protección de datos recoge los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) (…) vemos que la misma se encuentra estructurada pensando en bases de datos o listados de información obtenidos por las empresas para la realización de sus actividades comerciales. Es decir,* ***pareciera que nuestro legislador no se puso en el lugar que ocupan las redes sociales ni contempló la regulación de los datos proporcionados por los usuarios para su participación en las mismas*** *ni en los textos de las comunicaciones que circulan por Internet por plataformas como Twitter o Facebook*".

Corroborando lo señalado por Abel Revoredo y conforme a lo que sucede en nuestra realidad, el diario El Comercio describe en una noticia la cantidad de uso que hace nuestra población en Internet, señalando en su noticia de que los peruanos consumimos más internet que la media a nivel mundial, en una franja de edades que oscilan entre los 15 y 24 años de edad, del mismo artículo se puede detallar lo siguiente: **(s/a, El Comercio, 2014)** "...***el segmento de edad comprendido entre los 15 y 24 años el que más tiempo está conectado en la red***, (Fig. 1) con un 37,3% de la audiencia total, cantidad superior al promedio global que, en el caso de América Latina, alcanza el 33,4%. ***El tiempo promedio de los usuarios locales en la red es de 18.2 horas al mes***, mayor al registrado por sus pares de Venezuela, Colombia, Chile, México y Puerto Rico." **(s/a, El Comercio, 2014),** de lo expuesto, la preferencia en el consumo de la red, revela que ocupamos mucho tiempo en las redes sociales, veamos: "*El último estudio publicado por ComScore Perú no deja lugar a las dudas: los peruanos somos facebookeros y pasamos mucho más tiempo que el promedio regional entretenidos viendo quién publicó qué. Las cifras no mienten: Perú concentra 5,8 millones de usuarios online, de los cuales 5,1 millones tienen Facebook. Además, como si no fuera suficiente, el 97% del tiempo que nos conectamos (18,2 horas en promedio al mes) es para visitar a la chismosita blanquiazul*". **(Mendoza Riofrío, 2014)** (Fig. 2) En conclusión "*pasamos más horas en Internet que los colombianos, estamos por encima del promedio mundial en horas por visitante a las redes sociales y crecimos 17% el número de usuarios de la red mientras que Chile solo creció 9%*" **(Mendoza Riofrío, 2014)**. La cantidad de usuarios que navega en Internet se ha visto incrementado tanto por la forma de acceder que va desde un celular hasta una Tablet, como en el tiempo de consumo, es por ello que se dice que en nuestro país hay una mayor penetración de Internet y con ello un incremento en el tiempo que se usa la red, "*pero aún somos pura interacción social, según ComScore Perú*" **(Mendoza Riofrío, 2014)**

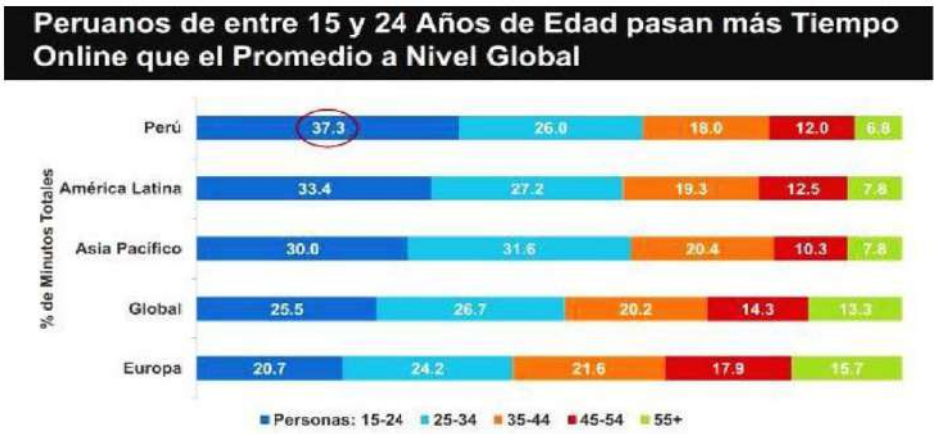


Fig. 1. Perfil de la audiencia Online en Perú *Fuente: Diario El comercio*

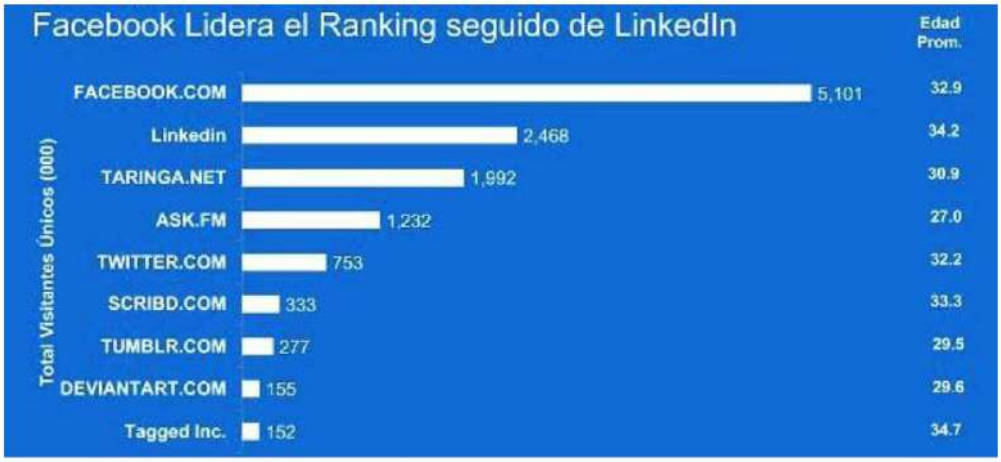


Fig. 2 Ranking de las principales redes sociales en Perú *Fuente: Diario El comercio*

Las cifras antes descritas, muestran que la cantidad de peruanos Online, en relación al resto del mundo son hechos que merecen una especial atención al momento de legislar sobre este tema, donde la intimidad y la privacidad superan el aspecto personal y privado de protección, para convertirse en una necesidad social que el estado debe regular.

En el plano internacional se puede referir situaciones más precisas que atentan contra la intimidad, tanto de personajes públicos, como de personas naturales, que debido a una normativa aislada, imprecisa y falta de sistematicidad, no responde a nuevas formas de violación a la

intimidad y convierte a cualquier ciudadano en víctima, veamos lo señalado por el diario ABC:

> "**La presidenta de Brasil Dilma Rousseff, una de las víctimas del espionaje norteamericano reveladas por el extécnico de la CIA Edward Snowden, empuñó el año pasado la bandera de un entendimiento global sobre los principios básicos que deben guiar a internet**. Una propuesta que lanzó en su último discurso ante la Asamblea General de Naciones Unidas. Bajo la batuta de Rousseff, Brasil aprobó el mes pasado una Carta Magna de internet, que ha sido ampliamente elogiada por especialistas de todo el mundo. **La carta también garantiza la privacidad de los usuarios, que al cerrar una cuenta, sus datos personales quedarán excluidos de internet.** Los datos pueden ser almacenados por seis meses en caso de investigación, pero después deben desaparecer. **Las empresas tampoco pueden grabar ni guardar informaciones sobre páginas visitadas.**" **(Goyzueta, 2014)**.

En concordancia con lo señalado, nuestra información se ve afectada en la red sin alguna normativa que defienda el interés de las personas tal como lo revela **(El blog salmon, 2013) ¿A cuánto venden Google, Facebook y otros la identidad y la información privada de sus usuarios**[1]?; Será cierto lo que sostiene Mark Zuckberg fundador de Facebook asegurando que las personas están conformes compartiendo sus vidas en la red **(bitelia, 2014)**, donde "**La idea de privacidad está muerta**", entonces para qué existe en nuestra normativa el Art 2. Inc. 6, 7 de la Constitución donde señala que los servicios informáticos no afecten la intimidad, añadido a ello y en contraste con sus unilaterales y cambiantes condiciones de servicio, entonces porque ***inician demanda***

[1] *"Usuario de Internet" (Universidad de Palermo, pág. 02), se refiere a la persona física o legal que está usando el servicio de acceso a Internet, y en esa capacidad tiene la libertad de impartir y recibir información, y utilizar u ofrecer aplicaciones y servicios a través de dispositivos de su elección. Cualquier persona legal que ofrezca contenido y/o aplicaciones en Internet también es un usuario de Internet*

colectiva contra Facebook por razones de privacidad **(fbclaim, 2014),** donde **más de 21000 personas se suman a esta iniciativa que involucra a más de 10 países de la comunidad europea**, ***cuestionando entre otros puntos la validez y eficacia del consentimiento sobre el uso de los datos de las personas*****, la vigilancia y el pase no autorizado de datos que muchas agencias de seguridad tienen sin informar a los usuarios;** ¿habrá necesidad de que los usuarios deban tener un mayor control sobre cómo los gobiernos y compañías usan sus datos? **Es concebible lo sostenido por** (**Edward J. Snowden, sobre la vigilancia de las agencias de seguridad estatales de Estados Unidos y Reino Unido.**) **(Correo/Agencias, 2013)** Donde **EE.UU. registró en secreto llamadas a través de la Agencia Nacional de seguridad (NSA) afectando a millones de personas, incluida la presidenta de Brasil**; habrá censura y persecución gubernamental a la tendencia moderna basada en la libertad y privacidad, de ello y en convergencia con los párrafos anteriores, solo hemos logrado la primera parte de la defensa de nuestras garantías fundamentales "la libertad", pero, ¿**Qué hay de la intimidad, privacidad y de los datos que de ella se generan? ¿Habrá algún alcance jurídico para solucionar esta problemática tan singular?**

En el ámbito normativo es de conocimiento que existen organismos e instituciones jurídicas que regulan aspectos aislados referidos a internet, tal es así que nuestro Código Penal, gracias a la ley de Delitos Informáticos se encarga de los ilícitos que tengan un soporte informático, tipificándolos como delitos, sin embargo a pesar de esta regulación jurídica no es posible iniciar un proceso, si no se configura un ilícito con todos los elementos de tipificación penal, entonces que sucedería si hay un Estado que espíe nuestra correspondencia o alguna organización de por medio, que violente, cometa ilícitos o permita que tengan lugar dentro de la esfera o espacio virtual conocido como Internet y que además no se encuentre en nuestro ámbito de competencia territorial, o no se conozca

al sujeto u objeto de imputación; bajo estas premisas ¿**Dónde y quién protege la Intimidad, privacidad y los datos personales de las personas**? ¿**Será posible resarcir estos hechos típicos**?

En otro punto de análisis, nuestra normativa establece el término de correo oficial de las personas, para realizar la notificación electrónica personal (ámbito privado), **pero no existe un proceso administrativo ni judicial para recuperarlo,** en caso de algún hackeo u otro ilícito, pues solo se condena el hecho a través de nuestro ordenamiento penal**, mas no se considera alguna forma de revertir el daño, por ejemplo reclamar ante la empresa prestadora de servicios, el que no se han vulnerado las condiciones de servicio por parte del usuario sino por un extraño,** d**onde está la neutralidad tecnológica que se halla en una ley y que no discrimina entre la información consignada sobre papel y la información comunicada o archivada electrónicamente, respecto a la privacidad que defiende la Constitución**.

Se usan bastantes avances tecnológicos pero su regulación y protección hacia el ciudadano es incierta y hasta se podría decir olvidada, ello se confirma con lo expuesto anteriormente, de lo cual no se cuenta con un sistema real y ajustado a las posibilidades del usuario, para accionar tanto judicial como administrativamente la defensa de sus derechos; **al respecto está la ley de protección al consumidor que se ve imposibilitada de actuar, pues no tiene alcances hasta Internet y sus aplicaciones** en el aspecto de la calidad de servicio y las cambiantes condiciones y términos de servicio que nos condicionan a aceptar en el momento que mejor les parezca a las aplicaciones de Internet **¿Se podría decir que es una aceptación legal o una pseudo aceptación? ¿Para aceptar realmente solo se necesita de un "clic"? ¿Cómo es posible reclamar ante este hecho?**, de otro lado se encuentra el "Reglamento de Calidad de los Servicios Públicos de Telecomunicaciones" del año 2005 que sentó las bases del principio de "Neutralidad de la red", pero solo de

acceso físico a Internet (cuyo organismo responsable de velar este precepto es OSIPTEL), **sin embargo no existe una normativa específica, respecto a los servicios virtuales o aplicaciones, a los cuales cada día más hacemos uso, vulnerando estos nuestros derechos básicos ante lo cual, nuestras instituciones legales no tienen alcance,** por ello, surge una última interrogante **¿es posible aceptar reiteradamente cambiantes condiciones de servicio que contravengan nuestros derechos constitucionales?**

1.2 DELIMITACIÓN DE LA INVESTIGACIÓN

A. Delimitación Social.

El presente trabajo abarca socialmente a todas aquellas personas o usuarios que puedan acceder a las aplicaciones de Internet.

B. Delimitación Espacial.

La presente investigación sobre la vulneración al derecho fundamental de la intimidad se establece específicamente en la ciudad de Arequipa – Perú, en el distrito de Paucarpata.

C. Delimitación Temporal.

Este trabajo investigativo, se desarrollará durante los años 2014 - 2015.

1.3 PROBLEMA DE INVESTIGACIÓN

A. Problema Principal

¿Por qué las aplicaciones de internet afectan el derecho fundamental a la Intimidad de sus usuarios en el distrito de Paucarpata, Arequipa 2014 – 2015?

B. Problema Secundario

1) ¿Cómo manejan las aplicaciones de Internet la intimidad de sus usuarios?
2) ¿De qué forma se vulnera la intimidad en las aplicaciones de Internet?

3) ¿Cómo proteger la intimidad de los usuarios en Internet?

1.4 OBJETIVOS DE INVESTIGACIÓN

A. Objetivo General

Analizar las aplicaciones de Internet que afectan el derecho fundamental a la intimidad de sus usuarios

B. Objetivos Específicos

1) Identificar el manejo que las aplicaciones de Internet dan la intimidad de sus usuarios.
2) Describir las formas de vulneración a la intimidad en las aplicaciones de Internet.
3) Determinar las formas de protección a la intimidad de los usuarios en Internet.

1.5 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Socialmente el problema se sustenta en la idea de que todo pueblo para encaminarse y desarrollar necesita de una base normativa, y los derechos fundamentales proclaman y resguardan a la persona en la Constitución Política del Perú, sin embargo en algún punto existen hechos que colisionan con uno o algunos derechos fundamentales y con ello las estructuras formales de la sociedad, en consecuencia, hoy se observa un uso cada vez más perverso de las nuevas tecnologías en menoscabo de la persona, tanto en la realidad física como en Internet, sin embargo, todos sabemos que los derechos fundamentales no son absolutos, tienen límites o presentan restricciones, pero, cuanto de lo garantizado, puede efectivizarse en un medio tan necesario e inseguro como es Internet, en caso de violarse alguno de ellos, por lo tanto el presente trabajo dará a conocer, si es viable económicamente para la persona afectada interponer un proceso constitucional para defender sus derechos en un servicio casi gratuito, se habrá alterado la naturaleza privada del servicio para dar lugar a una relevancia social de importancia general que merezca una respuesta legislativa para estos tiempos y los venideros.

Disgregando jurídicamente la problemática planteada, el presente trabajo pretende expresar y advertir existencia de una problemática relacionada con la Intimidad (privacidad y la protección de datos) en un sentido desproporcionado y no equilibrado o neutral, es decir, que defienda los intereses de las personas naturales y jurídicas en las mismas condiciones y con los mismos medios, debido a ello las aplicaciones que se ofrecen en Internet, no se adecuan a nuestra normativa pues no hay un ordenamiento que señale los parámetros de atribución a los que ceñirse, ello constituye un real perjuicio y detrimento a nuestros derechos, así, como un hecho común a toda la población, principalmente a la más joven que es la que hace un uso más intensivo de este medio y que no sabe ni puede ejercer debidamente sus derechos; ampliando este fenómeno, constituiría una problemática que afecta a todo el orbe, ya que la red es global y el acceso es local, es en ese punto de convergencia entre cada computadora u otro dispositivo y la red global en donde se producen los diversos fenómenos jurídicos que se han expuesto, ¿**porque no exigir a un servicio que se ofrece en Internet a respetar mínimamente nuestros derechos como personas, sin menoscabar sus intereses**? Un pensamiento contrario supondría parcialización y un atentado directo al estado de derecho.

Académicamente, muchos especialistas advierten la existencia de entes que atentan contra normas de carácter ontológico de la persona, por ello, el presente estudio desvelará que actualmente no solo una persona (natural o jurídica) aprovecha la necesidad y desinformación de las demás personas, sino que **existe toda una (maquinaria) taxonomía de entidades, países y otros organismos que hacen abuso de su poder para ejercerlo sobre personas desinformadas y desvalidas de un mecanismo jurídico sencillo, rápido y razonable que les garantice mínimamente el derecho fundamental a la Intimidad (privacidad y protección de sus datos personales,** ello señala que el legislador no

hace nada por cubrir ese vacío legal sin dejar ambigüedades, sumado a la inexistencia de un sistema de normas específicas que cautelen o defiendan nuestros derechos a nivel virtual o de servicios y aplicaciones informáticas, en consecuencia no hay quien controle la extralimitación de atribuciones de algunos servicios informáticos que por su características son determinantes para nuestra población, siendo la premisa de sus servicios "**acepto (todo y sin límites)**". Los servicios de redes sociales son una necesidad colectiva para la nueva generación **porque no regular estos problemas en una norma específica, no solo protegiendo la cotidianidad de las personas, sino que simplificando la forma de hacerlo, para que cualquier persona haga valer sus derechos equiparablemente con los que tiene una empresa, corporación o entidad que presta "servicios digitales"**, "Nada es gratis y no por una falacia debemos ceder ilimitadamente nuestros derechos fundamentales", no en vano se ha luchado tanto tiempo, para conseguir la normativa que nos respalda y garantiza lo que somos al día de hoy.

1.6 LIMITACIONES DE LA INVESTIGACIÓN

Señalando las limitaciones surgidas en el devenir del presente trabajo, se trae a mención la falta de apoyo de la universidad, pues cuenta con un engorroso sistema de normas internas que dificulta el acceso a los servicios bibliotecarios, teniendo en cuenta que una tesis necesita de un trabajo de acopio documental, ante lo cual la biblioteca se hace complicadamente inaccesible, pues el investigador tiene que verse forzado a pagar por el derecho de acceder a la biblioteca, sin importar si se es o no estudiante de titulación, cuando como estudiante, solo era necesaria la presentación del DNI y el "voucher" de estar al día en el pago de las pensiones, para acceder a la biblioteca.

En cuanto a la aplicación del instrumento y el recojo de datos, existió el inconveniente de que algunas personas no querían ser

encuestadas, debido a muchos factores, entre los que podemos citar, la falta de conocimiento, carencia de tiempo y el manejo superficial de sus derechos en Internet, pues algunas necesitaban preguntar sobre términos que conocían en la práctica, sin conocer su denominación técnica.

Por último, en la recopilación de trabajos similares al presentado, la universidad sin bien tenía trabajos que se relacionaban, ninguno presentaba de la problemática tratada.

CAPITULO II
MARCO TEÓRICO

2.1 ANTECEDENTES DE INVESTIGACIÓN

A. ANTECEDENTES HISTÓRICOS

Historia de Internet

Dentro del acontecer de uno de los avances más determinantes de los nuevos tiempos Internet como medio de comunicación es el más importante, en palabras de **(Pisanty Baruch, 2012, pág. 10)**, en relación al origen de Internet y su gobernanza, desarrolla que: "**Internet es una red de redes; un sistema de interconexión de redes de cómputo, que se ha extendido ya quizás a una sexta o incluso una quinta parte de la población mundial**. Las redes que se interconectan en Internet son redes que conectan computadoras y otros dispositivos en sitios tan diversos como...,...los hogares, las oficinas, los laboratorios y las fábricas"

Antes de Internet explica **(Alonso, 2011, pág. 8)**, "A mediados del siglo XIX, la prensa escrita europea informaba de los acontecimientos en el frente de batalla de la guerra de Crimea con varias semanas de retraso respecto a la fecha en la que ocurrían. Y era lo normal. Los sucesivos avances tecnológicos permitieron evolucionar hasta el actual diario de

papel que cuenta las noticias del día anterior. Y posteriormente a la radio y a la televisión, que cuentan lo que pasa y pueden trasmitir en directo, pero que suelen tardar algún tiempo (horas al menos) en empezar a cubrir cualquier acontecimiento no previsto...,... Internet le ha dado, una vez más, una nueva vuelta a este fenómeno de la aceleración de la disponibilidad de la información. En herramientas como Twitter la información está disponible desde el mismo momento en que se produce. Y, a menudo, trasmitida por los propios protagonistas o por testigos presenciales. Y retrasmitida (retwiteada) por multitud de individuos que hacen que llegue en cuestión de segundos a amplísimas audiencias."

El primer Internet

Pero como comenzó este fenómeno antes citado, **(Francés, 2006, págs. 3,4)** "Transcurría el 20 de octubre de 1969. Dos universidades de los Estados Unidos (Los Ángeles y Stanford), dos máquinas, una conexión. La meta enviar entre una y otra computadora la palabra "LOGWIN", "LOG" por conexión y "WIN" por victoria. Pero en ese viaje no todas las letras llegaron a su destino, las afortunadas fueron las tres primeras L-O-G, un hecho tal vez irrelevante para algunos; pero fue suficiente para demostrar que era posible que dos máquinas compartieran información. De ese experimento nació la primera red de computadoras, la llamada "ARPANET"."

Por su parte señala, **(Rubio Moraga, 2006, pág. 1)** "Todo comenzó con la creación del proyecto ARPANET (Advanced Research Project Agency Net) por parte del Gobierno estadounidense. **Se trataba de una red en la que los ordenadores conectados a ella disponían de diversas rutas por las que alternar las comunicaciones, con el fin de continuar funcionando aunque alguno de ellos fuese destruido como consecuencia de algún ataque**. Ya en los años setenta comenzaron a unirse a la Red empresas e instituciones educativas, desmarcándose así del ámbito estrictamente militar. De forma paralela iban surgiendo redes

similares a ARPANET a lo largo del planeta. Sin embargo, éstas no podían comunicarse entre sí, al utilizar protocolos para la transmisión de datos diferentes. Este obstáculo se salvó en 1974 cuando Vinton Cerf junto con Bob Kahn publicó el Protocolo para Intercomunicación de Redes por paquetes, en el que se detallaban las características del nuevo protocolo TCP/IP (Transfer Control Protocol/Internet Protocol), cuya definición como estándar culminó en 1982. La nueva especificación se concibió así como el idioma común de todos los ordenadores conectados a la Red. De este modo, diversas redes pudieron conectarse a una única, la cual pasó a denominarse Internet. Durante la década de los 80, la Red se expandió en gran medida gracias a la conexión de un gran número de ordenadores. Fue entonces cuando se creó el sistema de denominación de dominios (DNS, Domain Name System)."

El Internet como lo conocemos hoy en día

Una vez dado los acontecimientos antes citados hay que poner especial énfasis en los que nos relata **(Trigo Aranda, s/f, pág. 2)** "En 1982, ARPA declaró como estándar el protocolo TCP/IP (Transfer Control Procotol/Internet Protocol) y **es entonces cuando aparece la primera definición de Internet: conjunto de internets conectadas mediante TCP/IP**...Y nadie negará que esta definición, aunque correcta desde el punto de vista técnico, resulta bastante críptica para el personal no especializado.

Al año siguiente, 1983, el ministerio de Defensa USA consideró oportuno abandonar ARPANET y establecer una red independiente bajo su control absoluto (MILNET). De los 113 nodos que conformaban ARPANET en ese momento, 68 pasaron a la nueva red militar; a los restantes, se fueron uniendo cada vez más centros de todo el mundo"

Dicho lo antes citado, de alguna forma hay que conocer cómo funciona la red y que partes la conforman (Identificadores de Internet), el

autor **(Pisanty Baruch, 2012, pág. 13)**, refiere respecto a uno de ellos, el protocolo IP (tal vez el más importante) y un puerto asignado por el número 80, lo que sigue: "El protocolo IP o Internetworking Protocol, actualmente conocido también como Internet Protocol, es la base de Internet. Describe la partición de la información a transmitir en paquetes, y el enrutamiento de estos paquetes a través de puntos entre el origen y el destino. Puede ser concebido como un sistema que crea 65 535 "puertos", es decir, posibilidades de conexión entre computadoras. Cada puerto se asigna a una función diferente. Algunas funciones como las mencionadas en el texto tienen números de puerto fijos; otras seleccionan entre los puertos disponibles, o dentro de intervalos que pueden ser de cientos de números. Esta información evoluciona dinámicamente en el tiempo, conforme se inventan y estabilizan nuevas tecnologías en Internet"

Visto lo anterior, es necesario señalar su utilidad, para ello como señala **(Pisanty Baruch, 2012, pág. 14)**, "Cada computadora o dispositivo es identificado por una dirección numérica o dirección IP. En la versión vigente del protocolo IP, conocida como IPv4, estas direcciones numéricas se forman por cuatro tripletes de dígitos como, por ejemplo, 132.248.10.1."

Como se dijo, otro referente en el conocimiento de las partes que conforman Internet, son los Nombres de Dominio (DNS), a lo cual **(Pisanty Baruch, 2012, pág. 14)** define: "El Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) fue creado para facilitar la designación de recursos en las redes, con lo cual se evita la memorización de direcciones numéricas.

Es así que surgen los nombres de dominio que caracterizan a diversas organizaciones y a nuestras naciones los cuales son fáciles de reconocer por ejemplo .pe, .org, .br, uap.edu.pe, entre muchos otros,

(Pisanty Baruch, 2012, pág. 14) señala: *Los nombres de dominio son creados a solicitud delos usuarios (para este fin, "registrantes") mediante organizaciones comerciales o no lucrativas llamadas "registradores" y asentados en bases de datos operadas por "registros". En algunos casos, los registrantes hacen transacciones directamente en los registros", cada operación de los registros de una país en particular, tiene un régimen interior, donde se hace un registro de los datos referidos a direcciones IP y nombre de dominio DNS.*

Arquitectura tecnológica de Internet

Internet, como la red más grande conocida, está compuesto por una serie de computadoras, ordenadores y otros dispositivos que se unen y forman un complejo sistema de comunicación, debido a ello es necesario explicar con un poco más de precisión como está conformada físicamente, al respecto **(Gonzales, 2008, págs. 1-2)**, realiza una explicación muy concreta: "Como medio de transmisión internet usa en la mayoría de los casos la línea telefónica (de los diversos tipos que existen). Podemos decir que los ordenadores se organizan en tres niveles:

Usuarios finales. Son los ordenadores que usan los servicios de internet. Para enviar y recibir información de internet usan algún tipo de línea telefónica.

Ordenadores de los ISP. Un ISP es una empresa que nos permite acceder a internet, como Telefónica, Orange, ONO, Jazztel, etc. Estas empresas, en sus centralitas, tienen ordenadores y/o equipos que dan conexión a internet a los de los usuarios finales. Normalmente es la misma empresa con la que tenemos contratada la línea telefónica con la que accedemos a internet, pero puede ser otra (esto es por cuestiones comerciales y empresariales, más que técnicas).

Ordenadores servidores, que están constantemente encendidos y conectados y ofrecen los servicios propios de internet (páginas web, correo electrónico, transmisiones, mensajería instantánea, partidas de juegos on-line, etc.), que son accedidos desde los ordenadores de los usuarios finales.

Cada ordenador de usuario final está conectado a un ordenador de su ISP a través de la línea de teléfono. Los ordenadores de los ISP están conectados entre sí y con los ordenadores servidores, a través de las conexiones avanzadas de la red telefónica. Los ordenadores servidores también están conectados entre sí mediante las conexiones avanzadas de la red telefónica."

Principios básicos de Internet

Internet aparece como un fenómeno de corte transversal al igual que el medio ambiente, es decir nos afecta a todos, debido al carácter universal de su uso, sea por parte de nosotros o los que aún no lo usan, pero, algunos datos suyos están inmersos en esta enorme red internacional de la cual participa, sin embargo Internet no siempre tuvo el carácter universal del que hoy hablamos, **(Pisanty Baruch, 2012, pág. 11)** relata que: "El salto cualitativo que dio lugar a Internet fue un conjunto de ideas concebidas y puestas a prueba de manera experimental en los años de las décadas de 1960 y 1970, a saber, la conmutación por paquetes, **el principio "punta a punta" o end to end, la "inteligencia en la orilla"**, y la estandarización de las comunicaciones no al interior de todas las redes sino en la comunicación entre ellas.", del principio anteriormente citado surgen las bases técnicas, que hoy por medio del principio de neutralidad se puede valorar y regular normativamente.

Para que las tecnologías y los diversos adelantos pudieran comunicarse y entenderse, tuvieron que organizar protocolos o estándares que no solo permitieran la comunicación entre puntos, sino se

diera una comunicación rápida y eficaz, al respecto **(Pisanty Baruch, 2012, pág. 11)** explica que: "Los desarrollos tecnológicos fundamentales para el crecimiento de Internet se basaron en un principio también fundamental: la estandarización en la interfase y la interoperabilidad de las tecnologías. Para que la estandarización se diera de manera ágil y no interfiriera con el desarrollo de la tecnología, a diferencia de los procesos de la (UIT)[2] y de la ISO[3], los ingenieros productores de la tecnología se agruparon en la IETF[4] y dieron lugar al proceso de los RFC[5]."

Refiriendo un poco de los estándares anteriormente señalados, **(Pisanty Baruch, 2012, pág. 11)** señala como referente lo siguiente: "La (IETF) se volvió paradigmática de una amplia forma de conducir los asuntos de la comunidad, que fue reconocida como la "comunidad Internet".", término generalizado y manejado muy ampliamente, que modernamente da la idea de aldea global o globalización, esto es uno de los efectos más significativos que trajo consigo Internet.

Muy brevemente llegamos a otro momento muy importante dentro de la organización de Internet, **(Pisanty Baruch, 2012, pág. 12)** rescata: "Hacia 1995 la evolución de la IETF exigió la creación de la (ISOC), para contar con un paraguas corporativo que se hiciera cargo de operaciones como la organización de reuniones y publicaciones de la IETF; diera alojamiento formal a la función de editor de los RFC, y protegiera los estándares contenidos en éstos del riesgo de apropiación privada (desde un principio, y a diferencia de muchos otros procesos de estandarización, los estándares de la IETF han sido abiertos y gratuitos, para su libre adopción). De manera adicional, ISOC se estableció como una sociedad profesional para los especialistas dedicados a Internet como principal

---

[2] *Significa: Unión Internacional de Telecomunicaciones (UIT), http://www.itu.int.*
[3] *Representa: Organización Internacional de Estandarización (ISO), http://www.iso.int.*
[4] *Representa: Internet Engineering Task Force (IETF), http://www.ietf.org.*
[5] *Significa: Request for Comments (RFC).*

campo de acción, y como una sociedad para la promoción de Internet, su difusión global, y el conocimiento técnico necesario para expandirla."

Dentro de las diversas fuentes que se pueden tomar respeto a los antecedentes históricos referidos a Internet, se sabe que esta red es un medio que ha revolucionado las comunicaciones y hoy por hoy resulta determinante en la población mundial tanto su uso como su dependencia.

Gobernanza de Internet

En nuestros tiempos, hablar de comunicaciones inmediatas e informaciones en tiempo real, son cosa de todos los días, es allí donde Internet como la red de redes por excelencia prepondera muy por encima de los medios de comunicación tradicionales, pero a nivel jurídico empiezan a aparecer brechas que denotan la necesidad de regular este medio de comunicación multiangulado, un aspecto que se debe tomar en referencia es la gobernanza o aquella estructura jurídica destinada a coordinar acciones coherentes al marco jurídico nacional, por ello en un artículo de una revista digital mexicana, refiere respecto a los antecedentes de gobernanza en Internet lo siguiente:

> "Como se sabe, Internet es una red de redes; un sistema de interconexión de redes de cómputo, que se ha extendido ya quizás a una sexta o incluso una quinta parte de la población mundial. Las redes que se interconectan en Internet son redes que conectan computadoras y otros dispositivos en sitios tan diversos como, entre otros, los hogares, las oficinas, los laboratorios y las fábricas". "El salto cualitativo que dio lugar a Internet fue un conjunto de ideas concebidas y puestas a prueba de manera experimental en los años de las décadas de 1960 y 1970, a saber, la conmutación por paquetes, el principio "punta a punta" o end to end, la "inteligencia en la orilla", y la estandarización de las comunicaciones no al interior de todas las redes sino en la comunicación entre ellas." **(Pisanty Baruch, 2012, pág. 2)**

El término que refiere "*gobernanza de internet*" lo explica **(Pisanty Baruch, 2012, pág. 13)**, "gobernanza como lo cito al inicio del texto: **un**

conjunto de reglas, mecanismos y acuerdos que permiten la coordinación de una comunidad determinada. También tienen en común una característica sobresaliente: son mecanismos de gobernanza específicos para un dominio determinado, **reúnen a una comunidad específica y difícilmente pueden incorporar nuevos temas**."

Como páginas arriba se expresó, Internet cuenta con toda una arquitectura de conexión que recordando de manera resumida refiere **(Pisanty Baruch, 2012, pág. 5)**, "Si bien Internet es, como red de redes, un ente enormemente descentralizado, que permite la conexión de cualquier nueva red con la sola condición de que cumpla con los estándares de interoperabilidad y de que encuentre a un miembro de la red que le otorgue la conexión (en forma comercial o altruista), existen algunos pocos elementos que deben ser coordinados de una manera central: el Sistema de Nombres de Dominio; el sistema de asignación de direcciones numéricas o direcciones IP, y algunos parámetros técnicos."

Dado que la gobernanza reúne a una comunidad específica, este tema fue abordado con muchas inestabilidades en la Cumbre mundial de la Sociedad de la Información, lo cual es muy bien detallado por **(Pisanty Baruch, 2012, pág. 13)**, "A partir de la Cumbre del Milenio, la Organización de las Naciones Unidas (ONU) identificó que, junto con graves problemas a los que dedicaría sendas cumbres, como el agua y la salud y la pobreza, la humanidad, al llegar al tercer milenio de la era cristiana, había creado un área de oportunidad, el uso inteligente y apropiado de las tecnologías de información y comunicación (TIC), para dar paso a una evolución global hacia la Sociedad de la Información, como una etapa positiva de la humanidad."

Continuando con lo expuesto el autor Alejandro Pisanty señala:

> "El tema de la gobernanza de Internet en la Cumbre atrajo la condensación de múltiples corrientes de acontecimientos y sirvió como el campo en el que se desplegarían las rivalidades políticas

de diversos actores gubernamentales e intergubernamentales, además de los de la sociedad civil y los de las empresas. Muy temprano en la discusión se descubrió *el punto contencioso político clave en este tema: el papel asimétrico que juega el gobierno de Estados Unidos en la administración del DNS, que puede ser caracterizado bajo la bandera política de "control unilateral de la raíz"*. **Este tema sirvió de cobertura también al rechazo de China y otros países a la intervención extragubernamental en "asuntos de políticas públicas"**, que en realidad era una codificación para "política", y en forma específica, en el caso mencionado, expresaba una continua molestia por el reconocimiento internacional a la administración independiente del ccTLD .tw correspondiente a Taiwán. Bajo este título, el tema se polarizó, omitiendo los muchos otros tópicos en los que la Cumbre pudo haber producido acuerdos positivos La polarización sobre el DSF y sobre el tema de la gobernanza de Internet alcanzó tal intensidad que incluso en la fase de Ginebra, en 2003, la Cumbre no logró acuerdos, más allá del de continuar los trabajos hacia la segunda fase; en el segundo tema, mediante la formación del Grupo de Trabajo sobre Gobernanza de Internet (WGIG, por sus siglas en inglés),18 que definiera el tema; delimitara su alcance, y presentara opciones para que la Cumbre, en su segunda fase, estuviera en capacidad, de ser posible, de tomar decisiones. El mandato de la Cumbre al secretario general de la ONU era, además, que este grupo estuviera formado por miembros provenientes de los diversos sectores, explícitamente de "todos los stakeholders". La tradición se había invertido; donde antes la sociedad civil, el sector privado y los expertos pedían un lugar a la mesa, hoy eran los gobiernos del mundo los que buscaban asegurarse de no quedar fuera de la misma." **(Pisanty Baruch, 2012, págs. 20-21)**

Como se vio, para entender la gobernanza debe tenerse muy claro que son los llamados Stakeholders, por ello **(Pisanty Baruch, 2012, pág. 10)** explica: "Stakeholder es un término de difícil traducción. El término entra al debate a partir de dos raíces: Shareholder y "to have [something] at stake". En las compañías privadas Shareholders son accionistas ante los cuales la empresa y el Consejo Directivo de la misma tienen una obligación de rendición de cuentas. "To have something at stake" se traduciría castizamente como "que le vaya algo en ello", que se juegue,

que tenga algo en riesgo. De allí que en la constitución de ICANN se convocara a los *stakeholders, fueran éstos entes lucrativos o no, cuyos intereses fueran aceptados o cuyos principios fueran desafiados por la administración de los nombres de dominio y las direcciones IP*. El término sería transportado a la Cumbre Mundial sobre la Sociedad de la Información especialmente en los debates sobre la gobernanza de Internet."

Principales eventos de gobernanza de Internet en el 2014

El año 2014 fue muy relevante para la gobernanza de Internet. Durante ese año sucedieron una serie de acontecimientos sin precedentes que es posible que marquen un punto de inflexión en la gobernanza de Internet. Los más destacados han sido la celebración de la "Cumbre Mundial Multistakeholder sobre el Futuro de la Gobernanza de Internet" NETmundial, y el anuncio de la Administración Nacional de Telecomunicaciones e Información de Estados Unidos (NTIA) de su intención de transferir la custodia de las funciones de IANA a la comunidad global multistakeholder **(s/a, Foro de la Gobernanza de Internet en España, 2015)**.

Otros eventos importantes en 2014 han sido las tres reuniones anuales de ICANN, la novena reunión anual del IGF y la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones (UIT), que se celebra cada 4 años y en la que se elige el equipo nuevo de alta dirección de la UIT.

NETmundial

Con los sucesos ocurridos en 2013 y principios de 2014 sobre revelaciones que cuestionaban la seguridad, manejo y el modelo de gestión de la red, en 2014 surgió el movimiento NETmundial, que hasta ahora ha sido la cumbre multistakeholder más importante que se ha celebrado por el alcance y consenso alcanzados. NETmundial ha sido un

catalizador necesario para reanudar y reconducir el debate en torno a la Gobernanza de Internet. En esta cumbre se elaboró la "Declaración de São Paulo" que recoge una serie de principios generales para la gobernanza de Internet y una hoja de ruta para la evolución de la gobernanza del ecosistema de Internet. NETMundial se celebró en São Paulo, Brasil, durante los días 23 y el 24 de abril del 2014 cuyo principal objetivo fue redefinir el futuro de la gobernanza de Internet. Por esta razón concurrieron a este evento, miembros de más de 80 países de todo el mundo, cuya razón de asistencia fue la de representar a todas las partes interesadas en la gobernanza de Internet (modelo multistakeholder): gobierno, sociedad civil, academia, comunidad técnica y sector privado.

Al respecto la escritora **(Marty, 2014)** señala: "Internet cumple este año 25 años de vida y la cumbre NetMundial aprovechará la ocasión para *tratar temáticas en torno a la seguridad, gobernanza* ***y privacidad en la red***. Uno de sus objetivos es dar un puntapié inicial para desarrollar la mejor forma de regular la infraestructura y uso de Internet".

Uno de los factores que fueron concluyentes en la realización y desarrollo de este evento fue la 68 Asamblea General de Naciones Unidas celebrada en el mes de septiembre del 2013, donde la Presidenta Brasileña, Dilma Roussef, comprometió a los estados miembros a comenzar a regular y definir su papeles en un tema de suma importancia la gobernanza de Internet, en torno a la revelaciones hechas por E. Snowden y los excesos cometidos por la agencia de seguridad de EE.UU.

En correspondencia a lo expuesto líneas arriba, **(Marty, 2014)** señala: "Para Virgilio Almeida, secretario de política informática del ministerio de Ciencia, Tecnología e Innovación (MCTI) de Brasil, "puede haber puntos de tensión en la cumbre" en relación al papel que deben tener los Estados en la gobernanza de Internet. Se buscará consensuar entre las distintas posturas que existen hoy en día con países que

controlan absolutamente el contenido en línea (Cuba, China) y los actores que abogan por un Internet libre (Google), pasando por países como Argentina y el mismo Brasil, que han acusado a la Agencia de Seguridad Nacional (NSA) de Estados Unidos de conducir operaciones de espionaje informático en sus países.

A su vez y confirmando lo anterior **(Marty, 2014)** presenta: ""***Nuestra crítica está relacionada al hecho de que Internet depende de los Estados Unidos***. Los servidores raíz están todos en el hemisferio norte (Estados Unidos, Japón y Europa)", manifestó Bernardo Silva. Manifestó que luego de conocerse el caso de Snowden se produjo una reacción por parte del público en general y esto, según él, produjo la necesidad de emprender un cambio."

El efecto Brasil

Continuando un orden en las ideas, un aporte sustancial en la gobernanza de Internet, fue la creación brasileña en materia de regulación de Internet, es así que, "*El Senado de Brasil aprobó por unanimidad el martes un nuevo Marco Civil para la gobernanza de Internet en el país. La ley, que ha sido apodada "**La Constitución de Internet**"*, tuvo que deshacerse de algunos puntos polémicos para su aprobación final. Por ejemplo, a pesar de lo que buscaba el oficialismo brasileño, no se obligará a las empresas proveedoras de servicios de Internet a mantener un centro de datos en Brasil" **(Marty, 2014)**.

> En reacción a las revelaciones por el ex técnico de la CIA, E. Snowden, Brasil como país afectado por dichas declaraciones, tomó la iniciativa y aprobó el 22 de abril del 2014, la norma conocida como el "Marco Civil" de los derechos de los ciudadanos brasileños en Internet, estableciendo, derechos, garantías y deberes no solo para los ciudadanos sino también para las personas jurídicas que proveen de Internet a este país, este avance normativo como ya se mencionó líneas arriba, ha recibido

grandes elogios y hasta su sobrenombre es exclusivo "constitución de Internet", creando de este modo un pilar normativo en garantía al ciudadano y un acceso neutral respetando los derechos de la persona principalmente en de la privacidad, cuyo repercusión tuvo un efecto circunstancial en los documentos y creaciones que se concretaron a través de la NETmundial en la declaración de Sâo Paulo **(Marty, 2014)**.

La cumbre y la declaración de Sâo Paulo

El encuentro NETmundial concluyó con la presentación de la denominada "Declaración Multisectorial de São Paulo", versión final del documento resultante tras el debate. Esta declaración es un conjunto no vinculante de principios generalmente aceptados y una hoja de ruta que se anima a todos los interesados a seguir. Durante la sesión de clausura, en la que se presentó el documento final, Cuba, India y Rusia manifestaron públicamente su intención de no adherirse al documento por no estar de acuerdo en varios puntos del mismo que, según manifestaron violaban la soberanía de las naciones **(Marty, 2014)**.

La Declaración de São Paulo quedó dividida en los dos grandes apartados sobre los que versaron la Cumbre: "Los Principios del gobierno de Internet" y "La Hoja de Ruta para la evolución futura de la gobernanza de Internet" **(s/a, Foro de la Gobernanza de Internet en España, 2015)**.

El acuerdo de los nueve Principios:

En esta primera parte de la Declaración se identifica un conjunto de principios comunes y de valores importantes que contribuyan a la creación de un modelo inclusivo, multistakeholder, efectivo y legítimo y reconozca que Internet es un recurso global que debe ser gestionado al servicio del interés público **(s/a, Foro de la Gobernanza de Internet en España, 2015)**.

Los derechos que tienen las personas fuera de la Red también deben ser protegidos en Internet, de acuerdo con las normas

internacionales de derechos humanos, incluyendo los Pactos Internacionales de Derechos Civiles y Políticos y de Derechos Económicos, Sociales y Culturales, y la Convención sobre los Derechos de Personas con discapacidad **(s/a, Foro de la Gobernanza de Internet en España, 2015)**.

Se asume que los principios para la Gobernanza de Internet deben reflejar valores inalienables como la libertad de expresión, la libertad de asociación, la privacidad, accesibilidad, libertad de información y de acceso a la misma y de utilizar internet para el desarrollo económico **(s/a, Foro de la Gobernanza de Internet en España, 2015)**.

> Además, en los principios del documento se garantiza la protección de la limitación de responsabilidad de los intermediarios de manera que promueva el crecimiento económico, la libre circulación de información y la colaboración de todas las partes para combatir las actividades ilegales. Internet debe seguir siendo único, global e interconectado, basado en un conjunto común de identificadores que permita la libre transmisión de datos de acuerdo a la legislación vigente. La seguridad, estabilidad y resiliencia de Internet se identifican como uno de los objetivos fundamentales de todas las partes involucradas en la gobernanza de Internet **(s/a, Foro de la Gobernanza de Internet en España, 2015)**.

Principios del acuerdo de la declaración de Sâo Paulo

1) Derechos humanos y valores compartidos
2) Protección de intermediarios
3) Diversidad Cultural y lingüística
4) Espacio único y no fragmentado
5) Seguridad, estabilidad y resiliencia de Internet
6) Arquitectura abierta y distribuida
7) Principios del proceso de gobernanza de Internet
8) Entorno propicio para la innovación sostenible y creatividad
9) Estándares abiertos

B. ANTECEDENTES CIENTÍFICOS

La tesis propuesta por Daniel Arias Bustamante señala un principio básico en el entendimiento jurídico de la red y la protección de la intimidad, a continuación se detalla el resumen:

> El estudio del tema de la Neutralidad de la Red permite advertir que se trata de una materia que supone numerosos desafíos. Partiendo desde su propio concepto, encontramos diversidad de criterios; dicho aspecto se complica aún más, si **pretendemos definir los alcances de lo que representa una red neutral y propiamente la protección del principio de la neutralidad de la red;** todo lo cual obedece en parte al tan reciente origen y desarrollo histórico del tema en particular. **(Arias Bustamante, 2014)**

Extendiendo un poco el problema planteado, surge la necesidad de definir que es el principio de neutralidad en sí, puesto que ello está en especial relación con los derechos que pueda proyectar el usuario final o usuario de Internet, veamos:

> En términos generales, **el principio de la neutralidad de la red dispone que se debe dar un tratamiento igualitario y no discriminatorio en el acceso a las redes y sobre el tráfico que en ellas transita**. ***Ello implica que los operadores y proveedores no pueden bloquear, entorpecer o restringir arbitrariamente el derecho de los usuarios finales para acceder cualquier contenido en la red***, o utilizarla de cualquier forma que no resulte contraria al ordenamiento jurídico. La problemática y discusión central que gira en torno a la neutralidad de la red se puede resumir en las siguientes preguntas: ¿Se debe proteger el principio de la neutralidad de la red? Y especialmente: ¿Hasta qué punto debemos protegerla? ¿Cuáles son sus límites? **(Arias Bustamante, 2014)**

En respuesta a la problemática antes señalada, el citado autor propone.

> Como suele suceder, **corresponde acudir finalmente a "la ley" para brindar solución y definir grandes temas controvertidos como el presente; para lo cual en el presente**

> **trabajo, nos damos a la tarea de estudiar este principio desde distintos enfoques**, dirigiéndonos finalmente hacia la situación de Costa Rica. Partimos, en principio, de la premisa de que el marco normativo actual no ofrece una solución directa y concreta a esta controversia, aunque ciertamente nos podrá dar pistas respecto al camino más viable y armónico conforme a las políticas y el modelo regulatorio adoptado por el país. **(Arias Bustamante, 2014)**

Cómo proponer una norma que regule la neutralidad de la red si existen intereses encontrados al momento de crear parámetros en dicha cuestión, veamos:

> Mientras que **los defensores de los derechos de los usuarios finales y los proveedores de contenidos se postran como los grupos más importantes que apoyan la neutralidad de la red, los proveedores de servicios se oponen a este modelo. Unos buscan acceder a sus servicios plena e indiscriminadamente, al tiempo que los otros pretenden ejercer un mayor control sobre sus redes y maximizar sus ganancias**.
>
> La discusión **sobre la neutralidad de la red se puede relacionar con multiplicidad de temas importantes tales como: la calidad de los servicios, *los derechos de los usuarios finales***, el régimen de competencia, los derechos de autor, el régimen tarifario, la libertad de expresión, el desarrollo económico, el modelo de cobro de los servicios, entre muchos otros. **(Arias Bustamante, 2014)**

En correspondencia a lo citado, el autor de la tesis plantea a su realidad el principio de neutralidad, como se verá a continuación:

> La experiencia internacional, a la hora de tratar el tema, ha sido variada, aunque es claro que **la tendencia es proteger el principio; el meollo está en definir qué tanto protegerlo, y de qué modo. Estados Unidos y la Unión Europea se han visto envueltos en interminables discusiones que han resultado en "soluciones a medias", en la forma de disposiciones escuetas que carentes de verdadera coercitividad. Chile y Holanda fueron los pioneros que se lanzaron a regular la materia a nivel legislativo, demostrando así su total compromiso por instaurar y dar ejecutoriedad al principio de la neutralidad de la red. (Arias Bustamante, 2014, pág. 14)**

> En el plano costarricense, la aún reciente apertura del mercado de las telecomunicaciones hace difícil pretender contar a la fecha con regulación sobre una materia tan novedosa y particular. **El objetivo del presente trabajo es analizar el tema de la neutralidad de la red desde una perspectiva tanto general como específica. Tomando en cuenta la experiencia internacional y la situación actual del país**, se pretende llegar -en términos generales- a una posible solución sobre este tema para el caso costarricense. **(Arias Bustamante, 2014, pág. 14)**

> Como resultado de la investigación, se logró concluir que, aunque **existen multiplicidad de opciones para abordar el tema de la neutralidad de la red en el plano costarricense, la regulación a nivel de una resolución administrativa, por parte del Regulador que brinde cierto nivel de protección al principio de neutralidad de la red, representa de momento la opción más viable** a efectos de dar el primer paso hacia el ordenamiento y regulación de esta materia. **(Arias Bustamante, 2014, pág. 15)**

En la tesis presentada por **(Miranda Londoño, 2000, pág. 9)**, explica: **"**El Internet se desarrolla a una velocidad vertiginosa, que lo lleva siempre un paso adelante del derecho. **Es preciso que el derecho analice las nuevas realidades tecnológicas y los regule cuando sea necesario para proteger los derechos de las personas, en forma flexible que no limite los avances en la materia"**.

> Los paradigmas legales, sociales, económicos y políticos tendrán que ser revaluados. *Lo que ha sucedido hasta el momento con la aparición del Internet y las nuevas tecnologías que este trae consigo, es que distintos países han realizado un gran esfuerzo por promulgar nuevas leyes, que en su mayoría han tenido dos problemas fundamentales: La naturaleza cambiante de la tecnología tiene el potencial para dejar cualquier legislación sin efectos dentro de un período corto de tiempo. Además, los países han promulgado leyes desde una perspectiva nacional y es inadecuado gobernar de esta manera lo que es de verdad un problema global.* La construcción de esta nueva normatividad que proporcione una pronta solución a los vacíos legales existentes en

esta materia requiere gran exactitud y un alto grado de conocimiento técnico en sus construcciones teóricas y prácticas. **(Miranda Londoño, 2000, pág. 9)**

El presente documento pretende proporcionarle al lector una visión sistemática de los fundamentos legales necesarios para comprender la aplicación de temas como la tributación, jurisdicción, responsabilidad, aspecto probatorio, seguridad, comercio, propiedad intelectual e industrial en este nuevo mundo del Internet. En cada tema se hará una introducción de los aspectos técnicos de la materia y después, a través de la normatividad existente en el país, el derecho comparado y por medio de nuevas construcciones jurídicas, se buscará suministrar nuevas propuestas jurídicas para la reglamentación del ciberespacio en Colombia y el resto del mundo, ya que el Internet ha sobrepasado las barreras fronterizas y el esfuerzo normativo debe ser conjunto con otros países, para hacerle frente a esta nueva forma de realizar intercambio de bienes y servicios a través de la red. **(Miranda Londoño, 2000, pág. 9)**

Por último, el autor de la tesis **(Schubert Gallardo, 2012, pág. 3)**, presenta: "**Los reguladores de la tecnología se ven enfrentados a diversos problemas en su tarea. El primero de ellos es que se trata de temas técnicamente complejos** y de difícil acceso para muchos abogados, economistas y legisladores. Ellos preferirían que fuese algo de lo cual se ocuparan los expertos: ingenieros y técnicos".

El segundo problema en la regulación de la tecnología es la imposibilidad de prever los avances y cambios que vendrán en el futuro. La tecnología contemporánea se desarrolla velozmente de la mano de un mercado ansioso de innovación y el Derecho sólo avanza por incrementos espaciados en el tiempo a un ritmo -como señala John Perry Barlow- que sólo supera a la geología **(Schubert Gallardo, 2012, pág. 3)**.

Cualquier intento de regular por medio de métodos legislativos tradicionales materias que con su avance crean y destruyen constantemente paradigmas y realidades, convertirán rápidamente

en obsoletas las reglas que en un momento histórico dado sirvieron para normarlas y se corre el riesgo de limitar las posibilidades de desenvolvimiento futuro de la tecnología por medio de regulaciones que en el presente parecen adecuadas pero que en el futuro pueden resultar contraproducentes **(Schubert Gallardo, 2012, pág. 4)**.

> "En el caso de la regulación del principio de neutralidad de red en Chile y como bien señaló el diputado informante de la Comisión de Ciencias y Tecnología de la Cámara de Diputados al explicarle a la Sala el proyecto que se convertiría en la Ley 20.453: "el proyecto establece regulaciones sobre una materia compleja de explicar, porque es muy técnica. No obstante, constituye un gran salto que nos permitirá adecuarnos a las nuevas tecnologías."" **(Schubert Gallardo, 2012, pág. 4)**

> "La complejidad de un tema no es excusa para no entenderlo, sobre todo, considerando el impacto que Internet tiene sobre la economía del país y las posibilidades de comunicar, informar, de debate político e intercambio comercial que ofrece a los usuarios. En este sentido, el siglo XXI ha sido el escenario de una transformación radical en la forma de producir, distribuir y consumir información, conocimiento, cultura, bienes y servicios. **La tecnología moderna, y sobre todo Internet, han introducido cambios estructurales en los mercados tradicionales que es necesario que los reguladores tomen en cuenta" (Schubert Gallardo, 2012, pág. 4)**.

El presente trabajo tiene como objetivo general ayudar a superar al menos uno de los problemas enunciados: la complejidad técnica que presenta Internet para su regulación y explicar la necesidad de mantener los aspectos virtuosos de la Red. Para ello, el primer capítulo se ocupa de la relación que existe entre la regulación de la conducta humana y la tecnología. Explica que en ambientes que hacen uso intensivo de software, las posibilidades de actuación están condicionadas por el diseño del ambiente más que por las normas sociales o jurídicas, a diferencia de lo que ocurre en el mundo físico **(Schubert Gallardo, 2012, pág. 5)**.

Luego, el segundo capítulo analiza los hitos históricos que marcaron el desarrollo de Internet y explica los principios de diseño

que guiaron su construcción y que fueron responsables de darle a Internet su particular naturaleza descentralizada **(Schubert Gallardo, 2012, pág. 5)**.

Dentro de estos principios **el argumento End-to-End es de suma importancia ya que buena parte del debate acerca de la regulación de Internet por medio de la consagración legal de la neutralidad de red se ha guiado en base a esta regla. Ella señala que es en los extremos donde debe residir la "inteligencia" del sistema, mientras que la red propiamente tal debe limitarse a transmitir los mensajes que por ella circulan**. Este diseño es especialmente importante para el ambiente económico y competitivo que se genera ya que determina quienes y de qué forma participan en él **(Schubert Gallardo, 2012, pág. 5)**.

"El tercer capítulo resume las líneas generales del debate en torno a la neutralidad de red a nivel internacional para luego ocuparse de las razones que llevaron a la dictación de una ley que regula la neutralidad de red en Chile. El cuarto capítulo analiza en detalle, haciendo uso de herramientas económicas y jurídicas, la Ley 20.453 que modificó la Ley General de Telecomunicaciones (LGT), la cual hasta entonces ni siquiera contemplaba la existencia de Internet. Un tercer y último objetivo, del cual se encarga el quinto capítulo, es proponer líneas de acción que permitan aumentar el acceso y la competencia en el mercado de acceso a Internet, de modo que más personas puedan participar de sus beneficios" **(Schubert Gallardo, 2012, pág. 6)**.

C ANTECEDENTES EMPÍRICOS

El abogado Abel Revoredo en su artículo "Adolescentes y Redes Sociales", hace mención a la situación de abandono jurídico en la que se encuentran nuestros ciudadanos, ***pues somos los que mayor tiempo usamos Internet en el mundo para participar en una red social***, es así, que el autor realiza una crítica a nuestra flamante y recién entrada en plena vigencia ley de protección de datos personales, veamos: "*Si bien nuestra norma de protección de datos recoge los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) (...) vemos que la misma se encuentra estructurada pensando en bases de datos o listados*

de información obtenidos por las empresas para la realización de sus actividades comerciales. Es decir, ***pareciera que nuestro legislador no se puso en el lugar que ocupan las redes sociales ni contempló la regulación de los datos proporcionados por los usuarios para su participación en las mismas*** *ni en los textos de las comunicaciones que circulan por Internet por plataformas como Twitter o Facebook*" **(Revoredo, 2013)**.

El trabajo investigativo presentado por (López Herrero, López Moreno, & Galán Martín, señalan:

> "**Las redes sociales permiten al usuario generar un perfil con sus datos, y para ello ofrece un formulario animando a completar el mayor número de datos posibles: nombre, edad, sexo, foto, aficiones y gustos, formación académica, profesión e incluso orientación sexual**[6], de modo que toda ésta información se hace pública para todos los demás usuarios ya que por defecto, la accesibilidad del perfil no es sólo para tus amigos, sino también para las personas que forman parte de la lista de contacto de tus amigos. Es por ello que el propio concepto de red social conlleva a una cierta renuncia voluntaria a la intimidad en tanto que por el tratamiento masivo de información personal. ***Al menos el 40% de los usuarios de redes sociales tiene abierto el acceso a su perfil a todo el que pase por ellas, sin restricción alguna de privacidad***" **(López Herrero, López Moreno , & Galán Martín, 2010, pág. 7)**.

De otro lado los mismos autores señalan:

> "**Existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por cualquier persona**. Se desconoce en gran medida que los perfiles pueden ser archivados, facilitando la creación de bases de datos de personas con fines ilícitos y del valor que éstos pueden llegar a alcanzar en el mercado. **Por ello, se debe leer toda la información**

---

[6] *Se conoce como datos personales "El nombre, los apellidos, la fecha de nacimiento, la dirección postal o la dirección de correo electrónico, el número de teléfono, el número de identificación fiscal, el número de matrícula del coche, la huella digital, el ADN, una fotografía, el número de seguridad social, ...* ***son datos que identifican a una persona, ya sea directa o indirectamente***"

> **concerniente a la página web. En ella se explica quiénes son los titulares de la misma y la finalidad para la que se solicitan los datos**. Pero hay que destacar que **los mayores riesgos de los menores de edad está directamente relacionados con la proliferación de información personal gráfica de los menores publicada por ellos mismos o por terceros así como comentarios de naturaleza injuriosa que pueden ser delitos o faltas tipificadas en el Código Penal, con desconocimiento de la responsabilidad civil** por herir el derecho a la propia imagen del individuo como al honor. Éste es el caso del cyberbullyng en el cual se desarrollan conductas hostiles, se ataca la reputación, daña la intimidad a través de comentarios, se inventan historias, se crean perfiles falsos, suplantación de la personalidad, etiquetan fotos, insulta, amenaza, chantajea con subir fotografías, etc **(López Herrero, López Moreno , & Galán Martín, 2010, pág. 7)**.

A modo conclusivo y en concordancia a lo citado párrafos arriba **(López Herrero, López Moreno , & Galán Martín, 2010, pág. 7)**, "**Es por tanto esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada *si éstos no han autorizado expresamente su publicación***, pudiendo solicitar su retirada de forma inmediata. Luego **estas redes sociales deben establecer canales de denuncias, garantizando las respuestas en un breve plazo de tiempo, eliminando el comentario o la fotografía lesiva con la intimidad de las personas**."

Una opinión a destacar por su importancia y por definir aspectos muy precisos referidos a la intimidad y al usuario en internet en relación a las aplicaciones, explicando sobre las huellas que dejamos en Internet al navegar, mostrando la relevancia de los datos personales a una escala que trasciende a lo que nuestra normativa entiende, tal es así que con esos datos a los que no mostramos importancia debida, permiten a quienes los manejan crear "publicidad online comportamental", ***es decir venden nuestras preferencias en función a nuestra actividad online***, en base a datos que se fragmentan intencionalmente para evadir

normativas creando asimetrías de control de nuestra información que no se regulan, veamos:

> Cualquier actividad o consulta, que llevemos a cabo en internet, deja una huella o marca que permite nuestra identificación resultando casi inevitable que otros puedan acceder a esa información con un propósito (legítimo o ilegítimo) concreto. ***Esa huella personal permite la creación de perfiles online de los usuarios de internet, ya sea sobre la base de los datos que ellos mismos han suministrado acerca de sus gustos, preferencias, hábitos, información personal al consultar un sitio web*** (v. gr. Google, Amazon) o ya sea mediante su participación en una red social (v. gr. Facebook). Estos perfiles son creados normalmente, mediante un algoritmo, por terceros, a partir de la información recabada, tras la consulta de diferentes sitios web por los usuarios. **(Navas Navarro, 2015, pág. 1)**

En convergencia con la idea expresada anteriormente la misma autora acota:

> "Desde el punto de vista jurídico, una forma de intentar frenar esta asimetría, en cuanto al control de la información personal del usuario de internet, es la apuesta de la Unión Europea y del Grupo de Trabajo del art. 29 por un modo de exteriorización del consentimiento "opt-in" frente al modo de exteriorización, empleado en USA, conocido como "opt-out". Sin embargo, los diferentes sitios web, en sus filiales europeas, siguen empleando este segundo sistema en detrimento del primero. ***Al final quién toma las decisiones acerca del mejor uso a dar a la información personal no es su titular sino un tercero, el cual, puede llegar a obtener ingentes beneficios negociando con la información personal de los usuarios, a cambio de un precio***, en un "mercado secundario", si bien debería ser el titular de esa información quién decidiera libremente el uso más conveniente a dar a la misma, esto es, qué datos personales concretos permite que usen terceros de forma gratuita o a cambio de una contraprestación." **(Navas Navarro, 2015, pág. 2)**

(Cotino Hueso, 2011, pág. 386) Resume de su estudio: "**La colisión del derecho a la protección de datos personales y las libertades informativas en la red: pautas generales y particulares de**

solución", "El estudio fija la atención en el conflicto entre las libertades informativas y el derecho a la protección de datos personales, bajo la tesis de que el derecho a la protección de datos personales está sobreprotegido, ninguneándose el tradicional peso y protección constitucional de las libertades informativas. Ello no obstante se afirma que esta sobreprotección jurídica no tiene efecto alguno en la realidad. Y es que **en la red queda absolutamente indefenso el afectado en sus datos personales**, con lo cual ambos derechos y libertades quedan menoscabados. Se describe un análisis de supuestos y ponderaciones jurídicas realizadas mayoritariamente en sede de la Agencia Española de Protección de Datos. Se parte de que las libertades de expresión e información protegen la difusión de expresiones e informaciones y datos personales por cualquier sujeto a través de cualquier canal, modo o medio. Asimismo se afirman las pautas generales y particulares de resolución de conflictos de las libertades informativas y el derecho a la protección de datos. Finalmente se hace referencia al derecho al olvido en la red y la problemática de las hemerotecas digitales".

(Roig Batalla, 2011, pág. 44) En su artículo, **Tecnología, libertad y privacidad**, señala: "La tecnología garante de la privacidad, llamada PET o Privacy by design, está llegando a las recomendaciones de los grupos de expertos que asesoran a las Agencias nacionales de protección de datos. ***Si nos tomamos en serio la privacidad, deberemos convenir en la complementariedad de la tecnología con el Derecho como garantes de libertades***. La suma de ambas garantías coordinadas todavía sería mejor. Quizás el principio de privacidad en el diseño sea un primer paso en este sentido. En cuanto a las libertades informativas, la situación es distinta. **No hay aquí ninguna llamada a la protección tecnológica, ni siquiera limitada a un caso reducido o concreto.** La evolución tecnológica es en paralelo a la jurídica, y por el momento, las posibilidades tecnológicas se usan para clasificar y obtener significado relevante para un espacio complejo y que ha crecido sin orden

preestablecido: la blogosfera. El jurista debería acercarse sin complejos a esta propuesta multidisciplinar de estudio de las libertades informativas, si de verdad quiere complementar la protección jurídica de derechos fundamentales con el también apasionante mundo de la tecnología garante de los derechos fundamentales."

2.2 BASES TEÓRICAS

2.2.1 TEORÍAS Y MODELOS

A. Teoría del Estado Bienestar

El Estado benefactor, conceptualmente constituye el marco preciso para la construcción de un plan económico y político público "basado fundamentalmente en una economía pública que serviría para legitimar y brindar consenso respecto de las acciones de gobierno". **(Huerta Moreno, 2005, pág. 3)**

Así mismo concordando lo anterior, se puede agregar que la característica que definía al Estado bienestar era "***Promover reformas sociales, vinculadas a las garantías y los derechos ciudadanos establecidos en la Constitución***" **(Huerta Moreno, 2005, pág. 7)**

Historia del estado del bienestar. La historia del Estado del Bienestar se refiere a los orígenes y desarrollo del sistema económico, político y social, que, con posterioridad a la Segunda Guerra Mundial, se hizo ser común en los países desarrollados y de altos ingresos de la Europa Occidental, caracterizados por tener un sistema democrático, economías mixtas (combinando el libre mercado con aspectos de intervención o acción estatal en el estado del bienestar) y un sistema de garantías de acceso a beneficios sociales a la población en general. **(Wikipedia (C), 2015)**

Orígenes y evolución del término. El término Estado de Providencia fue acuñado bajo el Segundo Imperio francés por los republicanos que criticaban la filosofía demasiado individualista de ciertas leyes (como la ley Le Chapelier, que prohibía los sindicatos), y preconizaban un "Estado Social"; ***se preocupaban del interés de cada ciudadano y del interés general.*** **(Wikipedia (C), 2015)**

Sin embargo de lo expresado líneas arriba, la noción actual del término bajo análisis se explica con mayor detalle "La noción actual de Estado de providencia corresponde al término inglés de "welfare state" (*literalmente: "estado de bienestar"*), forjado en los años 1940. Esta última expresión habría sido creada por William Temple, entonces Arzobispo de Canterbury, como contraposición al warfare state ("estado de guerra") de la Alemania Nazi para describir la emergencia de las políticas keynesianas de posguerra" **(Wikipedia (C), 2015)**.

El sociólogo T.H. Marshall define el término como una combinación especial de la democracia, el bienestar social y el capitalismo. Algunos otros lo identifican, erróneamente, con el llamado Estado Social o incluso la Economía social de mercado. Para algunos, es el añadido de un Quinto poder del Estado: el de intervención económica, añadido a los tres poderes clásicos de Montesquieu y al cuarto poder, que son los medios de comunicación. Para otros, como Claus Offe, ***es un cambio profundo que nos permite hablar de un Estado Moderno***. **(Wikipedia (C), 2015)**

Antecedentes históricos generales del Estado del Bienestar

El sistema chino. Algunos de los desarrollos más antiguos de un sistema de estado de bienestar, a pesar de ser menos conocidos, fueron los que tuvieron lugar en el siglo XI en China bajo la dinastía Song. ***El Primer Ministro de la época en ese país, Wang Anshi, creía que es responsabilidad del Estado proveer a los ciudadanos de los***

servicios esenciales para un nivel de vida decente. Bajo su dirección, el Estado inició una serie de préstamos agrícolas y nombró comisiones a fin de regular salarios y planificar pensiones y jubilaciones para los ancianos y enfermos. Esas reformas fueron conocidas como Xin Fa o "Leyes Nueva". **(Wikipedia (C), 2015)**

Las Leyes de Pobres inglesas. En la Inglaterra de los 1600 se creó una legislación durante el reinado de Isabel I, conocida como leyes de los pobres en las que se distinguía tres clases de pobres, "Se introducen distinciones entre los "pobres discapacitados" (enfermos, ancianos, etc.), los "pobres capaces" pero que carecen de trabajo y los "pobres recalcitrantes". En general, se busca corregir en lugar de castigar. Se establecen Casas de Caridad, en las cuales los pobres incapaces recibían atención, y Casas de Industria, en las cuales los pobres capaces podrían trabajar, y, finalmente, se establece que los "recalcitrantes" serán enviados a prisión... ***La importancia de esta legislación es que introduce el concepto de la responsabilidad social por sus miembros***, no sobre una base religiosa, como anteriormente o en otros países" **(Wikipedia (C), 2015)**.

> Este es un sistema que, siguiendo una antigua tradición inglesa, se puede ver como basada en un "consenso político" que se estableció -o puede resumir- a partir de una frase que es común en Inglaterra: "***La verdadera medida de una civilización es la manera que trata sus miembros más débiles***", sentimiento que se empezó a hacer sentir en la política institucional durante la Época victoriana , por ejemplo, John E. E. Dalberg, Lord Acton, dijo: "La forma más cierta por la cual podemos juzgar si un país es realmente libre es la medida de la seguridad gozada por sus habitantes. **(Wikipedia (C), 2015)**

Estado social en Alemania.

En la Alemania del siglo XIX se desarrolla el primer sistema generalizado de protección social bajo el nombre de Wohlfahrtsstaat, que eventualmente evoluciono a lo que algunos han llamado "capitalismo no liberal" (en el sentido que no comparte las asunciones liberales acerca del mercado libre y algunas instituciones políticas) lo que, a su vez, está en las bases de un "estado del bienestar conservador" o "autoritario" **(Wikipedia (C), 2015)**

Este modelo se basa en una visión derivada de Kant que veía la ley no solo como el mecanismo de regulación de conducta ciudadana, sino también de cambio y progreso (en el sentido que regula cuando y en qué sentido el Estado debe intervenir en asuntos de interés común) **(Wikipedia (C), 2015)**

Estado del bienestar en el siglo XX

Así, dos modelos de estado de bienestar surgen: uno autoritario, basado en la expoliación de sectores que son percibidos como externos al país. El otro democrático, basado en la extensión real de los beneficios sociales a los miembros de la sociedad. El primero basado en la extensión a ultranza de la lógica de la competencia capitalista ***El otro, en la necesidad de mantener y extender, al menos en principio, los valores sociales y democráticos***.

Así se legitima, a nivel internacional, los principios de la intervención estatal en la economía con el fin de garantizar el bienestar general de la población y la estabilidad económica tanto de ellas como de los países. Siguiendo esas ideas muchos países, especialmente en Europa Occidental, abandonan las políticas de bienestar minimalistas anteriores y adoptan programas de provisión comprensivos. Con esas políticas, el Estado de Bienestar hace su "debut" en el mundo moderno.

Contexto económico político. Es en ese contexto que las aserciones tanto de Keynes (***Sólo el Estado "está en condiciones de restablecer los equilibrios fundamentales***", sea o no la intervención una medida aceptable en términos clásicos o en el largo plazo.) y Waligorsky - para quien tal intervención fue propuesta "como una resguardo contra el poder del mercado para socavar nuestras instituciones políticas y sociales más valuables... (...)...***un mercado totalmente libre es definitivamente no el mejor mercado para una democracia, un mercado sin regulaciones no garantiza ni justicia ni prosperidad***..." adquieren su verdadero significado. **(Wikipedia (C), 2015)**

Este es un momento definitorio en la política del siglo XX. Este fue el momento en que los conservadores cuyos principios van más allá que la defensa del Estado nación empiezan a buscar maneras de reformar las concepciones del liberalismo clásico, que se habían hecho comunes en esa corriente política, a fin de ***justificar intervención estatal en defensa de valores***.

JM Keynes economista que predijo una crisis, no sólo cuestiona los dogmas liberales, sino que provee una guía práctica de acción.

> "***Sólo el Estado tiene la capacidad de actuar en el interés general***", salvaguardando al mismo tiempo la democracia, sea o no la intervención una medida aceptable en términos clásicos o en el largo plazo. Se propone entonces la creación de las Naciones Unidas con la intención declarada de, entre otras, "crear condiciones bajo las cuales pueda mantenerse la justicia y el derecho internacional" y "promover el progreso social". Ese organismo, guiado por el espíritu keynesiano y aún en proceso de constitución, realiza en 1945, poco antes de finalizar la Segunda Guerra Mundial, una Conferencia Financiera en Nueva Hampshire (EE. UU.), que dieron lugar a los Acuerdos de Bretton Woods,

donde se decide crear el Fondo Monetario Internacional y el Banco Mundial. Poco después, en 1947, se firma el Acuerdo General sobre Aranceles y Comercio (GATT), antecesor de la OMC. **(Wikipedia (C), 2015)**

Sin embargo, con el paso del tiempo se nota que las políticas practicadas en los países europeos occidentales convergen en relación a dar un rol económico activo al Estado con el fin de obtener ciertos objetivos sociales comunes (tales como el bienestar social y Crecimiento económico) y se hace evidente que el progreso y estabilidad de cada país europeo depende de la de sus vecinos. Así, se crea un consenso que abarca desde los sectores más izquierdistas de los partidos socialdemócratas hasta los más derechistas o conservadores en los demócrata-cristianos. ***Ese consenso es lo que llegó a ser conocido como el modelo europeo de gobernanza, basado no solo en la idea que la sociedad -a través del estado- tiene una responsabilidad por sus ciudadanos*** sino también que el bien estar de cada uno, tanto para individuos como para países, depende del bien estar del vecino y que ese bien común, a pesar de visiones e intereses diferentes, puede lograrse a través de la práctica de la política de los consensos. Se empieza a hablar entonces de "la construcciones de comunidades". El resultado de todo lo anterior es lo que se conoce como el modelo del Estado de Bienestar.

Algunas autoridades van tan lejos como a sostener que el Estado de bienestar en realidad entra en crisis sin embargo sus mecanismos y logros aún se mantienen, en Europa, no solo como fundamento moral de cohesión social sino también como base realista y necesaria del arreglo socio económico común. Por ejemplo, a consecuencia de la Crisis económica de 2008-2009, la demócrata cristiana Angela Merkel -haciéndose eco del sentimiento keynesiano- proclamo "Solo el Estado es capaz de restaurar la confianza necesaria", y tanto el fabiano Gordon Brown como el conservador Nicolas Sarkozy han opinado que "el laissez-

faire tuvo su hora" e incluso The Economist, ese bastion del pensamiento liberal clásico moderno, ha dicho haciéndose eco el mainstream keynesiano "Para los liberales... la crisis ha puesto en relevancia defectos en la manera que ellos también implementan sus modelos. Lograr regulaciones adecuadas es tan importante como liberar los mercados; puede que un sector público eficiente cuente tanto como un sector privado eficiente, inversiones públicas en transporte, educación y salud, bien hechas, pueden pagar dividendos. ... pragmatismo y eficiencia siempre son de importancia" (The Economist,- editorial, edición del 9 al 15 de mayo de 2009). **(Wikipedia (C), 2015)**

B. Teoría sobre los derechos personalísimos

Sobre la naturaleza jurídica de los derechos personalísimos, existen dos posiciones, una que postula a la negación de que los derechos de la personalidad sean derechos subjetivos y otra que plantea lo contrario, a continuación se desarrollan ambas.

i. Teoría negatoria

Señala la página web **(Wikipedia (C), 2014)**:

"Alfredo Orgaz **niega el carácter de derecho subjetivo, para sostener que sólo son bienes jurídicamente protegidos o bienes personales que gozan del más amplio campo de protección jurídica**, puede inferirse propiamente derechos subjetivos".

A su vez el mismo Alfredo Orgaz, señala:

> "*No son derechos subjetivos porque estos en su estructura cuentan con un sujeto- objeto, y en los derechos de la personalidad se incurriría en un contra sentido, al identificarse el sujeto con el objeto la propia persona o el derecho habiente. El derecho subjetivo surge una vez que son lesionados los bienes de la personalidad, es sino el derecho subjetivo de la víctima a perseguir la reparación civil u obtener la condena penal del autor del daño*" **(Wikipedia (C), 2014)**

ii. Teoría de los derechos subjetivos

Explica **(Wikipedia (C), 2014)**, "sostiene que existe la posibilidad de lesionar, es porque hay algo que es objeto de esa lesión, y **ese algo, no es sino un derecho, en este caso inherente a la calidad de la persona del sujeto que la sufre, y que tiene por tanto un deber correlativo respecto de los demás que deben respetarlos**"

Dentro de las características que le son inherentes a los derechos personalísimos **(Wikipedia (C), 2014)** señala: "**son absolutos**, con una estructura formada por **un sujeto activo: su titular, un objeto: los elementos indisolubles de la personalidad: la vida, el honor, la integridad física, etc. y un sujeto pasivo: los demás miembros de la comunidad que deben de abstenerse de perturbar el ejercicio de ese derecho**."

C. Teoría de la privacidad por diseño o Privacy by Desing

(Roig Batalla, 2011, pág. 45) señala: "***La relación entre la tecnología y el Derecho es doble****: por un lado tenemos un estudio jurídico de un nuevo ámbito, como son las tecnologías de la información y las comunicaciones (en inglés IT Law; por Information Technology Law); por otro lado, tenemos la aplicación de recursos tecnológicos a problemas jurídicos (IT for Lawyers, por Information Technology for Lawyers)*".

La teoría propuesta trae consigo una innovación frente a lo vertiginoso del avance de las nuevas tecnologías en relación al avance del derecho, pues su implementación se consideraría una garantía a los derechos de los usuarios independientemente de la aplicación que usen y la condiciones que se le impongan, debido a que la presente teoría plantea desde un inicio el respecto de los derechos de usuario principalmente su privacidad en relación a los datos que se maneje,

veamos: **(Brian Nougrères, 2012, pág. 8)** "La noción de PbD[7] ***refiere tanto a una filosofía como a un enfoque por el cual la privacidad se encuentra integrada en el diseño tecnológico mismo***, consistente con la arquitectura del sistema de información y con el modelo de negocios. Se presenta como una forma de asegurar que la privacidad va a estar garantizada ante los cambios tecnológicos, que hoy por hoy se van sucediendo de manera cada vez más vertiginosa".

Esta teoría está enfocada en el usuario que hace uso de la tecnología, la misma que debe responder en correspondencia de modo positivo para con sus derechos, veamos: **(Brian Nougrères, 2012, pág. 4)** "...***privacidad a la medida del cliente, fue acuñado en la década de los noventa por Ann Cavoukian, Comisionada de Información y Privacidad de Ontario, Canadá***". Así mismo, **(Brian Nougrères, 2012, pág. 8)** señala: "*El concepto procura comprender el futuro de la privacidad.* ***De ahí que, más allá del cumplimiento de marcos regulatorios, la privacidad se entiende como un modo de operar de las organizaciones y de las empresas públicas y privadas***."

En apoyo a lo antes señalado, **(Vega Suarez, 2013)** señala: "*El origen de esta figura se remonta a los años 90, cuando una comisionada de información y privacidad de Canadá propuso su implementación en el diseño de diferentes tecnologías.*" Lo propuesta presentada sufrió un largo periodo de aceptación, hasta el año 2009 cuando su presencia se hizo imprescindible en la normativa de occidente siendo más precisos en la Unión Europea cuando se abordó el derecho fundamental de protección de datos personales, en concordancia con el avance tecnológico, es así que la comisión europea necesitó apoyo experto sobre la regulación del mencionado derecho, al respecto amplía: **(Vega Suarez, 2013) "**uno de los aportes del grupo de trabajo del artículo 29 fue la propuesta de innovación del marco con la inclusión de principios adicionales como el

[7] *PbD: Privacy by Desing o en castellano como privacidad por diseño.*

privacy by design (PbD) y el accountability. La consultoría tuvo como ejemplo un caso alemán, en donde la Corte Constitucional Alemana incluyó elementos del "PbD" en el fallo".

Como ya se vio un referente en la protección de la intimidad en la esfera que corresponde a la privacidad, está dirigida a la PbD o privacidad por diseño, la cual aparece como garante de los derechos de los usuarios al incorporar este derecho en la realización o diseño de las diversas aplicaciones informáticas en relación al derecho fundamental de la persona **(Roig Batalla, 2011, pág. 44)** señala: "*La tecnología garante de la privacidad, llamada PET o Privacy by design, está llegando a las recomendaciones de los grupos de expertos que asesoran a las Agencias nacionales de protección de datos.* ***Si nos tomamos en serio la privacidad, deberemos convenir en la complementariedad de la tecnología con el Derecho como garantes de libertades****. La suma de ambas garantías coordinadas todavía sería mejor.* ***Quizás el principio de privacidad en el diseño sea un primer paso en este sentido***."

Como se expresó, la teoría planteada nace en observancia a nuestros derechos fundamentales especialmente el de la privacidad, pues a estas alturas del desarrollo humano trasciende lo personal para convertirse en algo muy sustancial de lo humano, esto lo refuerza **(Brian Nougrères, 2012, pág. 4)** "si pretendemos preservar la privacidad (y nuestros derechos fundamentales), ***debemos enfrentar la situación con una nueva filosofía, desde una perspectiva integradora de la privacidad en la tecnología, y debemos hacerlo ya***. ¿De qué forma lograrlo? Introduciendo los fundamentos de la protección de datos en el sistema tecnológico de procesamiento de la información."

Dentro de los antecedentes que corresponden a esta teoría podemos citar a Ann Cavoukian, quien sentó las bases de esta teoría enunciándola allá por los años noventa como se vio un párrafo arriba, en

efecto, esta teoría tuvo amplia aceptación en 2010 durante la cumbre Internacional de protección de datos **(Vega Suarez, 2013)** "***El Privacy by Design fue incluido como estándar internacional en el marco de la 32a Conferencia Internacional de Protección de Datos y Privacidad***", incorporando la idea de mediar el derecho a la privacidad durante la realización o diseño de la tecnología, lo cual tuvo gran acogida y aceptación como se verá más adelante **(Brian Nougrères, 2012, págs. 4 - 5)** "***la concepción de Privacy by Design fue objeto de consideración por el comisionado europeo de Protección de Datos, quien realizó un llamamiento a los gobiernos a dictar leyes que rijan las nuevas tecnologías***, y motivo de mención por la CNIL, autoridad francesa de protección de datos en sus guías para la protección de datos personales. El término también apareció en la legislatura federal de los Estados Unidos de Norteamérica en abril del 2011, cuando se presentó el Commercial Privacy Bill of Rights".

Dentro de lo que enseña la realidad, existen diversos cambios que se viene implementando en nuestro país, uno de ellos y del que hacemos análisis y reflexión es el referido a la intimidad, privacidad y protección de datos personales y las diversas aplicaciones de Internet, esta situación la explica y ejemplifica **(Roig Batalla, 2011, pág. 45)**: "*Así, por ejemplo* ***las Agencias de protección de datos están reclamando en el campo de la privacidad en las redes sociales la aplicación de un principio nuevo: la privacy by design. Esta expresión alude a la protección tecnológica de la privacidad desde el mismo momento del diseño de la aplicación***." Situación que aún no se vislumbra en nuestro país, porque el legislador olvidó considerar a las redes sociales dentro de lo normado por la ley de protección de datos personales, entonces en que situación nos encontramos como usuarios.

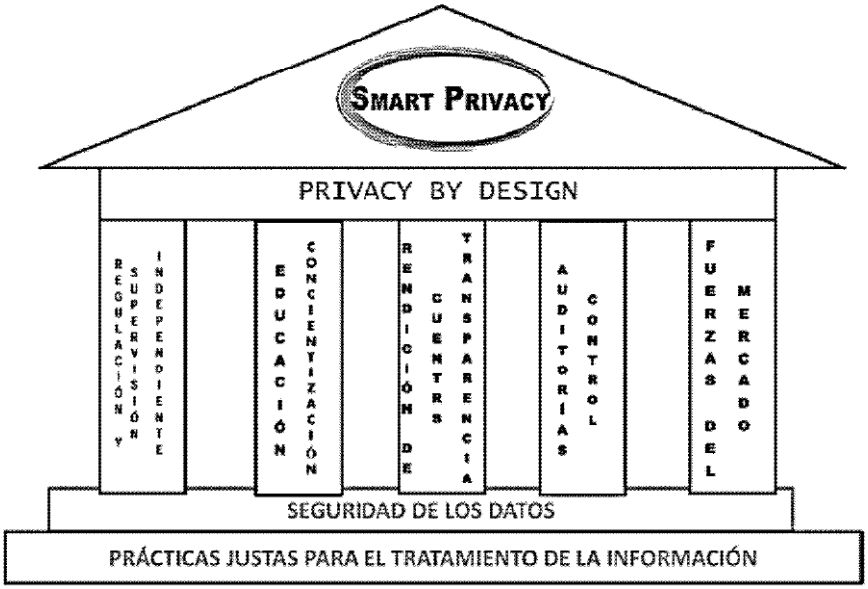
Esta situación ocurrió de manera similar en la Unión Europea durante la propuesta de su reglamento general de protección de datos, en

la que se incluía la citada teoría, sin que se quedara en claro los alcances de la misma y su aplicación, veamos: **(Vega Suarez, 2013)** "*El proyecto de Reglamento General de Protección de Datos de la Unión Europea incluye dentro de su articulado una opción denominada el Privacy by design, traducida como "la privacidad desde el diseño"*. ***La concepción de la idea es muy buena, pero una vez leída la propuesta de reglamento no queda muy clara su aplicación, pues no está desarrollada con la suficiente profundidad***."

La idea de considerar la privacidad en el diseño no se opone a la libertad empresarial en Internet, todo lo contrario, ofrece una gama de posibilidades y presenta soluciones a las variadas normativas con las que tiene que lidiar una empresa que presente un producto o servicio en Internet, al respecto **(Vega Suarez, 2013)** detalla: *"..."privacy by design"* ***debe ser entendida por las empresas como una herramienta con producción positiva de resultados, ya que la inversión en cumplimiento normativo posterior será mínima o tal vez innecesaria, porque tendrán en el mercado un producto/servicio, que se adecue a un estándar legal, con calidad y un excelente cumplimiento normativo****, lo que les permitirá competir en un mercado, sin pensar en inversiones de consultoría posterior relacionada con protección de datos, ofreciendo servicios adaptados a las necesidades del mercado".* Entendido lo expuesto sería la opción más inteligente por los empresarios del mercado de Internet pensar en lo que presenta la mentada teoría que ir corrigiendo las deficiencias legales que susciten su producto o servicio en Internet, **(Vega Suarez, 2013)** añade: "*Con lo que,* ***los empresarios deberán pensar en función de la protección de datos y de su cumplimiento normativo, desde la concepción de la idea de negocio y de esta manera ajustar su actuación con un carácter preventivo****, diseñando los parámetros necesarios para conseguir los objetivos del Reglamento: el respeto y cumplimiento del derecho de protección de datos*".

Un aspecto a tomar en consideración lo trae el término "***Smart privacy***" o privacidad inteligente, el cual trae consigo un conjunto de mecanismos orientados a garantizar los datos de los usuarios, esto combinado con la privacidad por diseño en las aplicaciones tecnológicas de comunicación, supondría un avance esencial para el futuro, ya que el acopio de datos personales es un hecho con el que tenemos que mediar de manera inteligente, **(Brian Nougrères, 2012, pág. 4)** considera: "***El mundo en el que vivimos hoy es un mundo en que la vigilancia se considera un insumo imprescindible para una vida armónica en sociedad, en que se procura información acerca de los individuos por todos los medios***, en que se producen perfiles de las personas según sus comportamientos, acciones que pueden llevarnos a asumir conductas discriminatorias."

En armonía con la teoría bajo explicación, se presentó el término "Smart privacy" o privacidad inteligente que como ya se dijo son un conjunto de mecanismos orientados a garantizar los datos o información de los usuarios, lo cual sumado a la teoría propuesta cuenta con una estructura que la estratifica sobre pilares, cada uno de los cuales se fundamenta en la protección de datos que más adelante se desarrollaran, veamos la ilustración realizada por *Anna Brian Nougrères*.



Fuente: Anna Brian Nougrères, traduciendo a Ann Cavoukian, Commissioner Ontario, 2009.

Desarrollando la gráfica propuesta tenemos en la base de la privacidad inteligente a las prácticas justas para el tratamiento de la información lo cual se expone: **(Brian Nougrères, 2012, pág. 5)** "...***lo que implica que la información personal debe ser recabada siguiendo rutinas de uso adecuadas***."

A continuación la misma autora explica sobre la segunda parte que corresponde a la seguridad de los datos veamos: "En un segundo escalón aparece la seguridad de los datos, ***como una exigencia justa que merece especial atención cuando refiere a asegurar la privacidad. Privacidad no implica seguridad. La seguridad tiene que ver con las prácticas de gerenciamiento de la información, desde el punto de vista del control.*** Aluden a proteger la privacidad contra ataques de terceros... **(Brian Nougrères, 2012, pág. 5)**"

Desarrollando lo traducido por Anna Nougrères en la figura anterior, tenemos un sistema que conforma lo que se presentó como "privacidad inteligente" cuyo primer pilar que se desarrollará corresponde a todo el ámbito normativo garante de los derechos de la sociedad, **(Brian**

Nougrères, 2012, pág. 6) "*La primera columna corresponde a leyes, normativa y supervisión independiente. Los tres elementos funcionan de manera reactiva, describiendo las consecuencias de cualquier falla en la protección de los datos personales. Tienden a actuar por detrás de la tecnología y por detrás de la sociedad*".

Consecutivamente a lo expuesto en el párrafo anterior se trae a mención un aspecto quizás transversal a todo problema no solo jurídico sino de otras índoles, con esto se hace referencia a la educación factor crucial en toda sociedad y determinante de su desarrollo en todo aspecto, ampliando ello **(Brian Nougrères, 2012, pág. 6)** señala: "A continuación está la columna educación y concientización. Como bien lo decía el filósofo griego Epictetus: "solo los educados son libres". ***En materia de privacidad tanto la educación como la concientización son claves para las empresas, para las organizaciones, para los consumidores***". Este párrafo a consideración personal, llega muy acertado para nuestra realidad, debido a que existen profundas diferencias en el aspecto educativo que se dan en nuestra realidad, tal es así, que hoy en día y posiblemente mucho después de que se escriban esta palabras, aún haya personas que desconozcan de la tecnología y su influencia en la educación, siendo por esto muy importante incorporar a la educación como un factor de apoyo para el debido ejercicio y aplicación de derechos que son garantía para el real desarrollo de la persona en nuestro país.

En tercer lugar, tenemos un aspecto que debe considerarse con especial cuidado y como un requisito del actuar de las empresas en la red, puesto que va dirigida a la transparencia con que opera una empresa en la red, **(Brian Nougrères, 2012, pág. 6)** establece: "*La tercera columna predica la transparencia y rendición de cuentas como buenas prácticas que son consideradas elementos de higiene organizacional*".

En lo que corresponde a la cuarta columna, tenemos lo referente a las funciones de un ente fiscalizador o regulador de los datos personales, que para efectos prácticos solo es posible de realizar con las empresas que operan dentro de nuestro país, desprotegiendo a las personas que por mayoría de uso frecuentan redes sociales y otras aplicaciones que no se encuentran dentro de nuestro país y son inmunes a controles u otros procesos análogos de control o transparencia respecto a los datos personales que recogen de usuarios peruanos, reforzando lo señalado tenemos a **(Brian Nougrères, 2012, pág. 6): *"La cuarta columna, auditorías y control, describe los procesos necesarios para asegurar la ejecución de la protección de datos personales en todo su ciclo".*** La privacidad tiene que estar desde un inicio, en función del control y el acceso de personas a los datos personales o privados, así como el tiempo máximo que se conservarán los datos personales.

En último lugar tenemos un factor del cual depende la aplicación de la teoría en desarrollo, con esto nos referimos a las fuerzas que operan el mercado digital, de las cuales depende en qué medida adoptan los recaudos necesarios para ejercer su actividad de negocio en la red, es así que finalmente, se trae a mención a una de las partes que más controversia plantea en el mundo digital, los empresarios y el comercio electrónico en relación con la seguridad de los datos personales y privacidad de sus clientes, **(Brian Nougrères, 2012, pág. 6)** plantea: "*La última columna trae a colación las fuerzas del mercado. Así se trate de empresas que hagan negocios por Internet, o no, es innegable que los consumidores cada vez se vuelcan más hacia el comercio electrónico.* ***Aquellas empresas con contingencias que afectan los datos personales de sus clientes, con seguridad verán disminuir el valor de su marca y sufrirán una desventaja con respecto a las demás***".

Es de acuerdo a lo tratado líneas arriba, que se disgrega el concepto de "Privacidad por diseño" pues se encuentra por encima de lo

ya referido como un factor integrador de las características señaladas en cada uno de los pilares que se han citado, finalmente **(Brian Nougrères, 2012, pág. 6)** comenta: *"Por encima de estas columnas está el concepto PbD que asegura la protección de los datos personales, integrado con las especificaciones del diseño de las tecnologías de la información del medio físico y de las prácticas del negocio".*

Atendiendo a lo señalado por la teoría bajo desarrollo la "privacidad por diseño", **(Roig Batalla, 2011, pág. 50)** señala: "*El primer ámbito en el que presumiblemente se aplicarán será el de la protección de menores frente a los riesgos derivados de la participación de éstos en las redes sociales.*"

En la misma vertiente de lo ya dicho anteriormente, se hace referencia a los menores de edad que participan desde muy temprana edad, en uno de los mayores desafíos que plantea la red al ámbito jurídico "las redes sociales", es en tal sentido, es válido señalar la opinión:

> "Si tenemos en cuenta que la edad a la cual los menores frecuentan las redes sociales está disminuyendo, hasta los primeros contactos sobre los nueve años, se comprende la problemática subyacente y la aceptación, aunque sea a regañadientes, de la entrada de la tecnología en este supuesto. Sin embargo, los riesgos son múltiples, ***y si nos tomamos en serio la privacidad, deberemos convenir en la complementariedad de la tecnología con el Derecho como garantes de libertades.*** La suma de ambas garantías coordinadas todavía sería mejor. Quizás el principio de privacidad en el diseño sea un primer paso en este sentido. **(Roig Batalla, 2011, pág. 50)**

Respecto a las ya aludidas "redes sociales" podemos señalar conclusivamente que son las personas quienes determinan cuanto de sus derechos han de ser respetados, sin embargo muchos de ellos parecieren no conocer de los mismos en un primer momento, sin embargo esto tiene un trasfondo más social, pues importa saber más de los otros que preocuparse de lo que sucede conmigo, es así que la libertad de

gestionar nuestros derechos esta en nosotros y la ley debe ser quien apoye esta decisión de un modo más protector, pues que sucedería si ocurriera un epidemia de suicidios y el Estado dejara de hacer algo al respecto, veamos un atisbo final de privacidad por diseño en las redes sociales:

> "Somos los propios usuarios los que tenemos que gestionar esta privacidad en los ajustes de la red social en la que creemos un perfil. De esta forma existen dos formas de privacidad dentro de las redes:
>
> - Privacy by design: es la posibilidad para que el usuario defina el alcance de los contenidos que publica frente a terceros.
> - Privacy by default: es la práctica de los prestadores de servicios que por defecto, y sin que los usuarios realicen ninguna acción, da las máximas garantías en materia de privacidad. Garantía para que el usuario se encuentre en un entorno de confianza". **(Viera Lozano, 2014)**

Consideraciones en torno a la privacidad en las aplicaciones de Internet

La privacidad como configuración predeterminada

(Brian Nougrères, 2012, pág. 10) Partimos de la base de que lo primero que se genera son las configuraciones que han sido predeterminadas teniendo en cuenta la especial valoración del elemento privacidad.

(Brian Nougrères, 2012, pág. 10) El sistema se genera con total certidumbre, previendo desde el inicio la privacidad, razón por la cual no hay opción posible de que la configuración no preste a los elementos de protección del dato la debida atención y consideración ni es posible que el usuario del sistema pueda actuar con error aplicando un parámetro que contradiga los elementos básicos de la protección del dato personal.

Privacidad integrada en el diseño

(Brian Nougrères, 2012, págs. 10-11) El concepto de PbD se presenta integrado en el diseño y la arquitectura de los sistemas de tecnologías de la información y en las prácticas de negocios.

(Brian Nougrères, 2012, págs. 10-11) Lo referente a la protección de datos no está agregado al sistema, no está superpuesto al sistema ni es un anexo al mismo. Es un componente esencial del sistema: su núcleo funcional.

(Brian Nougrères, 2012, págs. 10-11) Se presenta holísticamente, esto es, abierto a los nuevos contextos que puedan surgir, como factor de integración e interacción de los distintos intereses involucrados y, además, en una forma por demás creativa, por cuanto se prevé la necesidad de autoinventarse a sí misma cuando no existan otras alternativas viables.

Respeto por la privacidad del usuario

La idea de PbD es mantener todo el sistema centrado en el usuario. Tanto los arquitectos como los operadores tienen la responsabilidad de proveerle de fuertes esquemas de privacidad por defecto, que recaben el previo consentimiento y fortalezcan las soluciones que son amigables para el usuario.

En general, se entiende que los mejores sistemas son los que han sido conscientemente diseñados con especial atención a las necesidades de los usuarios, que son los primeros interesados en manejar su propia información.

Otorgar al usuario la posibilidad de jugar un rol activo en la manipulación de sus propios datos puede constituir un chequeo muy efectivo contra malos usos y abusos de la protección de datos personales. Para ello, el usuario debe otorgar su consentimiento en forma libre y específica, y poder controlar la veracidad de la información, a cuyos efectos debe proveérsele de acceso a dicha información, así como de los

medios de reclamo en casos de verificarse inexactitud en sus datos. Tanto las soluciones técnicas como las operaciones de negocios y las arquitecturas físicas de las redes, en fin, todo el sistema debe proveer al usuario de un grado tal de consideración que lo coloque en el centro de las operaciones de acopio de datos personales.

D. Teoría del consentimiento informado

Desde los aportes de la medicina en al ámbito jurídico se presenta una teoría que servirá de sustento, al presente trabajo investigativo en lo referente a la aceptación o consentimiento en las aplicaciones de Internet en relación al derecho constitucional de la Intimidad.

La teoría del consentimiento informado es de origen anglosajón, específicamente al sistema norteamericano, aunque después ha pasado a formar parte del patrimonio ético de casi toda la práctica médica occidental. "Si bien su gestación tiene mucho que ver con el propio modelo ético-político con que aquel país vio la luz a finales del siglo XVIII, su verdadero desarrollo hay que situarlo en el contexto del amplio movimiento de reivindicación de los derechos civiles que, iniciándose a finales de la II Guerra Mundial, tiene su auge en la década de los sesenta-setenta -y que tampoco se limita sólo a los EE.UU-". **(Simón Lorda & Concheiro Carroba, 2014)**

Del mismo modo, **(Ávalos & Tapia M, 2013)** conceptúa la teoría de la siguiente manera: "El consentimiento informado es la aceptación racional por parte de un paciente de una intervención médica o la elección entre cursos alternativos posibles."

De lo citado, la parte que interesa rescatar es aquella referida a la capacidad o potestad de la persona de elegir los medios, alternativas u otros recursos que considere en su libertad y su grado de conocimiento para con su salud, que para nuestro caso en particular serviría para

establecer, cuáles son los alcances del consentimiento sobre la cesión de sus diversos derechos y la necesidad de negociar sobre los mismos entre el usuario y las diversas aplicaciones que se usan en Internet.

El aspecto medular a tomar en sustento, se guía por lo señalado a continuación: *Para que un «consentimiento» se considere aceptable no sólo debe de ser «libre», sino también «informado», lo que quiere decir que tiene que ser emitido tras un proceso de evaluación de una determinada cantidad de información relativa a la decisión a tomar.* **(Simón Lorda & Concheiro Carroba, 2014)**

Ante lo señalado en el parágrafo anterior, las aplicaciones de Internet, precisan de obtener el consentimiento para hacer uso en todas las formas posibles y con el mayor ingreso económico a costa del usuario que "cede" mediante un "clic" *ilimitadamente sus derechos*, aún si estos tienen relevancia constitucional o están protegidos en una ley, no informando al usuario sobre los derechos que se verán involucrados, los grados de libertad que tendrán respecto a esos aspectos que derivan de sus derechos constitucionales en la red y el grado de cosificación que se le atribuirá a la persona en las mencionadas aplicaciones.

Del mismo modo se puede señalar otra idea que sustenta la teoría abordada "*no existe garantía de que algo, por el mero hecho de ser aceptado por la comunidad científica, sea necesariamente ética o legalmente aceptable*." **(Simón Lorda & Concheiro Carroba, 2014)**

Las empresas o aplicaciones que se ofrecen en Internet, propugnan a una especie de desgobierno legal, en el sentido de que si una persona se conecta de una ubicación, sea nuestro país por ejemplo, no intenta compatibilizar o amoldar su modelo de negocio como cualquier empresa lo haría en cualquier país, muy por el contrario, obliga al usuario a sujetarse a una normativa extranjera, sin importar que legalmente y

éticamente se vulneraría los derechos de la persona, por negarle, en un atisbo del problema, un derecho de defensa ante cualquier controversia, entre otros, es decir que la red para estas organizaciones económicas si tiene una regulación jurídica, pero que no se adapta, ni aplica a todas las personas que hacen uso de ellas, extendiendo la idea, abusan de la libertad y coaccionan con la necesidad de la persona para sujetarse a las condiciones que se le impongan, sin derecho a reclamo u otro.

> *«El consentimiento informado consiste en la explicación, a un paciente atento y mentalmente competente, de la naturaleza de su enfermedad, así como del balance entre los efectos de la misma y los riesgos y beneficios de los procedimientos terapéuticos recomendados, para a continuación solicitarle su aprobación para ser sometido a esos procedimientos. La presentación de la información al paciente debe ser comprensible y no sesgada; la colaboración del paciente debe ser conseguida sin coerción; el médico no debe sacar partido de su potencial dominancia psicológica sobre el paciente.»* **(Simón Lorda & Concheiro Carroba, 2014)**

Ante lo señalado, cada persona que cabalmente o no, hace uso de las diversas aplicaciones en Internet, desconoce los alcances del consentimiento que prestó al suscribirse en determinada aplicación de Internet, inobservando las aplicaciones de Internet el balance legal con el usuario, sin embargo aquello no agrupa la real dimensión del problema, sino, contradictoriamente a lo que se piensa solo es el inicio de los sinsabores jurídicos respecto a los derechos del usuario, pues no se le indica o se hace saber cuál es la trascendencia de sus derechos a futuro, por otro lado y más importante aún es el hecho de que la mayoría de aplicaciones en un intento de "mejorar" la experiencia del usuario cambian unilateralmente la condiciones y términos del servicio, nuevamente sin mencionar nada sobre todos los derechos del usuario, sin que haya un consenso entre la aplicación y el usuario, es decir o aceptas o aceptas, sino adiós y sin reclamos; no se estará presentando información sesgada, coercionando al usuario y claramente sacando ventaja de su potencial

dominancia sobre los derechos del usuario, dicho esto no sería factible aplicar a las aplicaciones el uso del consentimiento informado sobre los derechos de los usuarios en Internet.

Según la teoría presentada, la limitación de la libertad puede presentarse de tres formas posibles:

Persuasión. En este caso, quizás el más frecuente de todos, el paciente es sometido a un procedimiento sin darle la oportunidad de que efectúe ningún tipo de elección **(Simón Lorda & Concheiro Carroba, 2014)**, "puede darse en forma no deliberada por parte del médico, o en forma implícita por el efecto psicológico del médico y su conocimiento" **(Ávalos & Tapia M, 2013),** extrapolando la situación, se podría afirmar que esta es la situación que cotidianamente sucede en Internet en lo relativo a la aceptación de los términos y condiciones contractuales en las diferentes aplicaciones de Internet.

Coacción. Una decisión está tomada bajo coacción cuando la persona está amenazada por otra de forma explícita o implícita. La coacción será tanto más potente cuanta mayor diferencia exista entre el poder del coaccionador y el del paciente, puesto que a mayor poder de aquél, mayor credibilidad tendrán sus amenazas para éste. **(Simón Lorda & Concheiro Carroba, 2014)**, así ejemplifica **(Ávalos & Tapia M, 2013)** "*situación que puede suscitarse como amenaza implícita o explícita de pérdida de beneficios y derechos*"

Manipulación. El médico, ***por sus conocimientos e influencia psicológica, se encuentra en una posición respecto al paciente que le capacita para presentarle la información de tal manera que le empuje a tomar una decisión determinada***. **(Simón Lorda & Concheiro Carroba, 2014)**, apoya a lo señalado anteriormente, **(Ávalos**

& Tapia M, 2013) "puede darse al entregar información sesgada y/o distorsionada".

Se podría sintetizar que las aplicaciones de Internet con mayor uso, conocen, manejan (por así decirlo) tendencias sociales para obligarnos a usar una determinada aplicación en función de las necesidades comunicativas de cada usuario aprovechando los vacíos legales o el desconocimiento del usuario para lucrar con nuestra información.

Los ámbitos que debería abarcar la información proporcionada, tal y como lo entiende la teoría del consentimiento informado estadounidense, en el ámbito médico son los siguientes:

- Descripción del procedimiento propuesto, tanto de sus objetivos como de la manera en que se llevará a cabo.
- Riesgos, molestias y efectos secundarios posibles.
- Beneficios del procedimiento a corto, medio y largo plazo.
- Posibles procedimientos alternativos con sus riesgos, molestias y efectos secundarios respectivos, y explicación de los criterios que han guiado al médico en su decisión de recomendar el elegido en lugar de estos.
- Efectos previsibles de la no realización de ninguno de los procedimientos posibles.
- Comunicación al paciente de la disposición del médico a ampliar toda la información si lo desea, y a resolver todas las dudas que tenga.
- Comunicación al paciente de su libertad para reconsiderar en cualquier momento la decisión tomada **(Simón Lorda & Concheiro Carroba, 2014)**.

A modo autointepretativo y llevado a la realidad bajo análisis, se puede sugerir los siguientes ámbitos que podrían aplicarse al ámbito

digital en consideración a lo señalado anteriormente, en relación al consentimiento para que sea informado veamos:

1. Descripción – resumen de los términos relacionados a la intimidad y otro derechos en cuanto a los objetivos o fines de recojo de información así como el destino que tendrán luego de recogidos.
2. Riesgos que supone una eventual aceptación de las mencionadas condiciones.
3. Beneficios que resultarían de aceptar las condiciones de las políticas de privacidad en términos del derecho a la intimidad.
4. Alternativas de no aceptarse las cambiantes condiciones de políticas de privacidad.
5. Comunicación – posibilidades de la información, es decir sugerir cambios con un tiempo razonable para tomar una decisión adecuada a las posibilidades sugeridas.
6. Libertad para escoger, se entiende que al cambiar el sentido de las políticas de privacidad se cambian los términos contractuales de uso de un determinado servicio, ello debe darse en igualdad de condiciones para negociar y plantear alternativas beneficiosas a los usuarios en respeto de sus derechos en consonancia con los derechos de la persona jurídica que proporciona determinada aplicación en Internet.

Este principio rescata dos cualidades que dotan de mayor seguridad al consentimiento, estos son la validez y la autenticidad.

El concepto de validez tiene mucho que ver con la intencionalidad de las acciones, la cual está muy condicionada por el estado anímico del sujeto. Por ejemplo, una decisión tomada durante un ataque de ira puede no ser válida aunque el sujeto la adopte voluntaria, informada y competentemente, porque seguramente no refleja de forma adecuada sus deseos. **(Simón Lorda & Concheiro Carroba, 2014)**

La autenticidad por su parte tiene que ver con las escalas de valores. Una decisión tomada por un sujeto voluntario, informado y competente pero que va en contra de la escala de valores que esta persona ha defendido a lo largo de toda su vida, puede no ser en realidad auténtica. **(Simón Lorda & Concheiro Carroba, 2014)**

Esta plantea un argumento para sustentar la necesidad de información de la que se debe dotar a un usuario, en una aplicación de Internet que maneje información personal o íntima del mismo, así tenemos:

"*El médico tiene un privilegio terapéutico que le capacita para ocultarle información (al paciente) respecto a los riesgos del procedimiento al que va a ser sometido*". **(Simón Lorda & Concheiro Carroba, 2014)**

De manera análoga, por sus conocimiento técnicos las aplicaciones de Internet cuentan con un privilegio de especialista (técnico) que los capacita para ocultar información, hacerla ambigua, poco entendible o ininteligible, por ello, la norma debe dotar de igualdad para quitar esta asimetría tanto de derechos como de información.

Por último y conclusivamente la mencionada teoría se resume en lo siguiente: "***cada paciente tiene unas necesidades distintas de información, especialmente los que tienen creencias idiosincráticas o peculiares, un comportamiento sanitario fuera de lo habitual, una historia personal o familiar característica o alguna otra circunstancia de este tipo***». *Este criterio implica, por lo tanto, que si un médico tiene fuertes razones para creer que su paciente desearía conocer un determinado riesgo, aunque él personalmente no lo considere de importancia «material», tiene la obligación de comunicárselo*. **(Simón Lorda & Concheiro Carroba, 2014)** Esta es la razón por la que se ha tomado en consideración la teoría antes descrita, pues, cada persona en

sus distintos sistemas de valores, debe tener la posibilidad de elegir determinadas decisiones en el total de sus características o tan solo en parte, ello en el aspecto digital se conoce como autodeterminación informativa, al cual toda persona está facultada, sin embargo a nuestra normativa le falta algunos atisbos de refuerzo a los derechos de los ciudadanos o en este caso usuarios sin menoscabar los intereses de las personas jurídicas en un clima de respeto mutuo, así mismo, esta teoría trasciende a la propuesta personal, por el hecho de que las personas al momento de manejar su derecho humano a la intimidad basada en su dignidad como persona, supera a una decisión simple o común, si esta información va a ser aprovechada por una empresa que trabaja con los medios sociales suficientes, que pueden hacerla difundible o no y la posición de las empresas que en este caso son las aplicaciones de Internet, merece especial atención por la relevancia social que implica en cualquier comunidad especialmente la nuestra que hace un uso intensivo de Internet especialmente en aspecto referente a las redes sociales

E. Teoría de los Seis Grados de Separación

Las redes sociales online son servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información personal de uno. La teoría base de las redes sociales es detallada por **(López Herrero, López Moreno , & Galán Martín, 2010)** "Se fundamenta en la "Teoría de los Seis Grados de Separación" de Karinthy en 1929, **la cual afirma que cualquier persona puede estar conectada a otra del planeta a través de una cadena de personas que no supera los seis intermediarios**. Así, en 1998 nace SixDegrees y en el 2002 Friendster, a partir de aquí comenzarían numerosas redes sociales cuyo auge comienza en el 2003. Las redes sociales pueden ser de dos tipos:

1. ***Generalistas***: buscan facilitar las relaciones personales y de ocio Ejemplo: Facebook

2. ***Profesionales***: fomentan las relaciones entre profesionales. Ejemplo: LinkedIn.com".

Un planteamiento más minucioso de la mencionada teoría la presenta:

> "La teoría germinal del desarrollo de plataformas para la creación de Redes Sociales en Internet parte de la teoría de los Seis Grados de Separación. Esta teoría fue expuesta mediante intuición inicialmente en el año 1929 por el escritor Frigyes Karinthy dentro de un relato corto denominado Cadenas. Según la teoría del escritor, el número de conocidos de una persona crece exponencialmente siguiendo un número de enlaces de una cadena que serían las relaciones humanas. De este modo, sólo sería necesario un pequeño número de enlaces para conectar cualquier persona con el resto de la población humana. Los intentos para tratar de demostrar esta teoría de una forma científica han resultado numerosos. En la década de los años 50, los investigadores del MIT y de IBM, Ithiel de Sola Pool y Manfred Mochen respectivamente, trataron de encontrar y demostrar el número de pasos necesarios para que toda la red humana estuviese interconectada. Pero ***no fue hasta 1967, cuando el sociólogo de la Universidad de Harvard Stanley Milgram trató de comprobar la teoría realizando un experimento que se fundamentaba en el envío de cartas postales. Teniendo presente que una red social comprende a un conjunto de gente con un patrón de interacciones entre ellos, Milgram diseño un experimento en el que trató de que una serie de sujetos dispersos geográficamente (Primero en Omaha, Nebraska y posteriormente en Wichita, Kansas) intentasen enviar una carta a un compañero suyo en Boston. La condición consistía en que a las personas que enviasen las postales debían conocerlas personalmente. Además, uno de los objetivos consistía en que las cartas llegasen lo más pronto posible y una vez que las cartas comenzaron a llegar a su destino, Milgram trazó su recorrido y la red de contactos, llegando a la conclusión de que eran necesarios seis pasos para interconectar a cualquier persona dentro de Estados Unidos".*** **(Ros Martin, 2010, pág. 2)**

A pesar de haber sido formulada en 1929, dicha teoría no contaba con mucha aprobación en el ámbito digital, hasta que se puso esfuerzo y especial énfasis para demostrarla, así explica:

> "A pesar de no poder demostrar la teoría de forma matemática, se han desarrollado numerosos conceptos a partir de ella como el popular Número de Erdös o, el más recientemente, en el libro Six Degrees: The Science of a Connected Age[8] del sociólogo Duncan Watts. En este libro, Watts, profesor de la Universidad de Columbia, expone el experimento que llevó a cabo **en el año 2001 cuando intentó repetir la comprobación de Milgram aunque para esta ocasión el medio utilizado fueron correos electrónicos**. De esta manera, Watts envió un correo electrónico en el que urgía que fuese reenviado por los destinatarios a sus contactos para comprobar cuánto tardaba en volver al primer emisor. **Finalmente, el mensaje fue reenviado a 48000 personas a lo largo de 157 países, lo que llevó al investigador a aventurar que la media de intermediarios entre una persona cualquiera y otra a nivel mundial era de seis** (Raghavan, 2002)". **(Ros Martin, 2010, pág. 2)**

F. El principio de supremacía constitucional

La Supremacía Constitucional ***es un principio teórico del Derecho constitucional que postula, originalmente, ubicar a la Constitución de un país jerárquicamente por encima de todo el ordenamiento jurídico de ese país, considerándola como Ley Suprema del Estado y fundamento del sistema jurídico***. Según cada país los tratados internacionales ratificados por el país gozan de igual rango (rango constitucional) o superior a las leyes e inferior a la constitución. **(Wikipedia (D), 2014)**

Desarrollo por países

Argentina

El Art. 31 de la Constitución Argentina versa: "esta constitución, las leyes que en su consecuencia el Congreso dicte y los tratados con las

[8] *Se traduce como: Seis grados: La ciencia de la era de la interconexión*

potencias extranjeras son la ley suprema de la nación". Este artículo establece la supremacía de la Constitución sobre leyes, reglamentos, actos administrativos y sentencias de los Poderes constituidos.

"La pirámide jurídica en Argentina quedaría con la Constitución y los Tratados sobre Derechos Humanos de jerarquía constitucional en la cima, los demás tratados internacionales inmediatamente después..." **(Wikipedia (D), 2014)**"

México

El Art. 133 de la Constitución Política de los Estados Unidos Mexicanos establece. "Esta Constitución, las leyes del Congreso de la Unión que emanen de ella y todos los tratados que estén de acuerdo con la misma, celebrados y que se celebren por el presidente de la república, con aprobación del Senado, serán la ley suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados".

"Los tratados internacionales celebrados por el Estado mexicano, en materia de derechos humanos, se ubican en el mismo peldaño que la Carta magna y por encima de las leyes expedidas por el órgano legislativo". **(Wikipedia (D), 2014)**

Perú

El artículo 51º de la Constitución Política del Perú señala que: "***La Constitución prevalece sobre toda norma legal; la ley, sobre las normas de inferior jerarquía, y así sucesivamente.***" En tal sentido ***este precepto constitucional se impone a todos los peruanos***, la primacía de la Constitución y la ley, según el cual se debe obediencia plena a la Constitución Política del Estado.

Venezuela

El artículo 7 de la Constitución de la República Bolivariana de Venezuela del año 1999, expresa que: "La Constitución es la norma suprema y el fundamento del ordenamiento jurídico. Todas las personas y los órganos que ejercen el Poder Público están sujetos a la Constitución" indicando así, la Primacía de la Constitución y la sumisión al derecho de las personas y órganos del Poder Público Nacional. ***La constitución de Venezuela presenta la particularidad de que ante un eventual atentado a la misma, en referencia a su vigencia, cada ciudadano está facultado para reinstaurar su plena vigencia***, veamos:

> "El artículo 333 de la Constitución: se refiere a la Rigidez de la Constitución Venezolana que no perdería su vigencia por ningún acto de fuerza o por cualquier otro medio distinto al previsto en ella. Dice textualmente así: "*Esta Constitución no perderá su vigencia si dejare de observarse por acto de fuerza o porque fuera derogada por cualquier otro medio distinto al previsto en ella. En tal eventualidad, todo ciudadano investido o ciudadana investida o no de autoridad, tendrá el deber de colaborar en el restablecimiento de su efectiva vigencia*"." **(Wikipedia (D), 2014)**

Control de Constitucionalidad

Para que el Principio de Supremacía Constitucional sea efectivo precisa de la existencia un mecanismo que lo garantice, a este mecanismo se lo conoce como Control de constitucionalidad así lo corrobora **(Wikipedia (D), 2014)** "juntos son dos de los más importantes pilares de la teoría constitucional. Para el desenvolvimiento de este control puede emplearse una Magistratura Constitucional y un Procedimiento Constitucional, elementos a través de los cuales se realiza el control de la vigencia del principio de constitucionalidad, o bien realizárselo en base al mecanismo conocido como sistema difuso de control de constitucionalidad, que puede estar a cargo de cualquier juez, sin importar su jerarquía o fuero".

G. Doctrina de la responsabilidad civil compartida

El estado como garante y protector de los derechos fundamentales debe tomar la iniciativa, ante supuestos que vulneren dichos derechos, para que una vez ocurrido el daño, si este no se puede reparar y/o hacer responsable a alguien, este trate mediante algún mecanismo de reparar dicha situación permitiendo a la persona recuperar lo que le fue arrebatado con el daño causado, esto constituye un precepto legal que en el ámbito jurídico se conoce como "*alterum non laedere*", es decir no dañar al otro, este principio surge del hecho de vivir en sociedad, "*el no causar daño a los demás es quizá, la más importante regla de las que gobiernan la convivencia humana*" **(López Herrera, 2004, pág. 1)**, así el derecho no busca proteger a quien produce un daño a otro, muy por el contrario, hace nacer un compromiso o una obligación, en la que el que causa un daño debe resarcir la situación a lo más parecido posible de cómo se encontraba antes de sufrir el daño.

Fundamentos filosóficos

> Para Kant la doctrina del derecho (doctrine of Right) enfoca hacia el aspecto externo del ejercicio de la libertad y tiene como principio a la máxima "***actúa externamente de manera que el uso de tu libertad coexista con la libertad de todos en concordancia con una ley universal***". Esta doctrina es la que da sustento a que ciertas obligaciones morales son también obligaciones legales cuyo cumplimiento puede ser obtenido coactivamente. **(López Herrera, 2004, pág. 2)**

> La concepción de Aristóteles al igual que la de Kant es igualitaria y basada en la igualdad absoluta de la dignidad de todos los hombres por el solo hecho de ser seres racionales libres. Aristóteles es el creador de las expresiones conmutativa o correctiva y distributiva para designar a los dos tipos de justicia...(...)...La justicia distributiva para Aristóteles tiene que ver con la interacción de los individuos y el estado, y se basa en la sola condición de la persona como integrante de la comunidad, abarcando potencialmente a todos los individuos. Los recursos o

> bienes existentes en la comunidad deben ser distribuidos de manera igualitaria en proporción al mérito o a las necesidades. Se relaciona la justicia distributiva con un aspecto positivo a tener acceso a esos recursos. En materia de daños esto tiene numerosas aplicaciones, por ejemplo quien causa un daño por incurrir en actividades riesgosas pero socialmente útiles, debe responder de los daños que causa aunque no se demuestre su culpa (responsabilidad objetiva). Es este tipo de justicia el fundamento también de la responsabilidad por el hecho de otro, conocida en el common law como respondeat superior o vicarious liability **(López Herrera, 2004, pág. 2)**.

La justicia conmutativa o correctiva, en cambio tiene que ver con la interacción entre individuos y sin tener en cuenta su posición relativa en la sociedad, méritos, riqueza o poder. ***Si una persona afecta o amenaza los recursos de otra a través de una acción que es incompatible con el principio de la absoluta e igual libertad***, ***la segunda tiene derecho a un reclamo contra la otra.*** Al revés de la justicia distributiva, la justicia conmutativa se relaciona con un aspecto negativo que da derecho al individuo a que nadie interfiera en sus derechos. ***Este tipo de justicia se corresponde claramente con la función compensatoria*** **(López Herrera, 2004, pág. 3)**.

Fundamentos económicos

Una respuesta que refuerza el fundamento anterior lo encontramos en el análisis económico del derecho que hace **(López Herrera, 2004, pág. 3)** "*es posible analizar las reglas jurídicas en consonancia con las económicas, y demostrar en la mayoría de los casos su eficiencia económica y en los casos en que esto no sucede, proponer su reformulación*".

A que se quiere llegar con lo dicho anteriormente, por un lado llenar el vacío legal producido cuando no cumple los requisitos para configurar el tipo penal cuando subsiste un hecho que dañe a una persona y ante ello el Estado debe intentar resarcir el daño causado a la persona, si se

pudiere, de otro lado suplir la normativa ante hechos de naturaleza lesiva a la intimidad cuya solución no este equiparada dentro de la naturaleza económica del perjuicio (honor, imagen, privacidad y datos personales), además y en concordancia con lo ya señalado, una persona no va a invertir una cantidad de dinero en la mayoría de los casos por un servicio casi gratuito que le perjudicó y que para reclamar, deba activar todo el aparato judicial, el cual a modo de crítica y conocimiento social es lento, necesita de una economía variable para sustentarlo y accionarlo además de no contar para estos casos en específico con una vía procesal delimitada en los casos que afecten la intimidad de forma muy diversa.

Frente a lo dicho es meritorio plantear un sistema jurídico que haga frente a futuras formas de violación a la intimidad que involucre al proveedor de aplicaciones de internet a participar en la normativa nacional de forma específica y garante de los derechos de la persona entre ellos la intimidad, coordinando acciones que hagan de Internet un sitio más seguro confiable y con similares características de apertura a las que tenemos hoy, es decir, un internet abierto pero que genere confianza en los usuarios que lo visiten a través de aplicaciones confiables, la respuesta está en unir privacidad, transparencia y usabilidad para generar confianza en los usuarios

Otro punto a señalar es el tema de neutralidad jurídica donde se permita al usuario tener las mismas potestades que la empresa o persona que le permite usar determinada aplicación, pues el consentimiento en este punto debe tener y tomar mayor preponderancia, cómo es posible ceder un derecho fundamental, sin posibilidad de reclamo, dicho en términos jurídicos, por qué se permite la indefensión en internet.

Por último se debe hacer mención a nuestra medida constitucional que protege la intimidad por excelencia el hábeas data que para expresarnos en los términos señalados líneas arriba, se queda corto tanto

en actuación, alcance y economía, pues dicha garantía constitucional no busca resarcir el daño sino cesar un acto que como sabemos en Internet no dura más que algunas fracciones de tiempo ante el cual esta garantía no tiene razón de ser, además de que no está preparada y facultada para abordar una tema que supera los límites nacionales, entonces no hay garantía que proteja.

2.2.2 BASES HUMANAS

A. La dignidad humana

"*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación, toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*"

Declaración Universal de los Derechos Humanos Art. 12

El manual de derechos humanos **(s/a, Derechos Humanos Manual para Parlamentarios, 2005, pág. 1)** define: "los derechos humanos ***son derechos que tiene toda persona en virtud de su dignidad humana***", así mismo:

> *Los derechos humanos son los derechos más fundamentales de la persona. Definen las relaciones entre los individuos y las estructuras de poder, especialmente el Estado. Delimitan el poder del Estado y, al mismo tiempo, exigen que el Estado adopte medidas positivas que garanticen condiciones en las que todas las personas puedan disfrutar de sus derechos humanos.* **(s/a, Derechos Humanos Manual para Parlamentarios, 2005, pág. 1)**

Los derechos humanos vistos desde la esfera supranacional presentan una connotación muy propia, tal es así que: **(s/a, Derechos Humanos Manual para Parlamentarios, 2005, pág. 1)** "**Los gobiernos y otros titulares de deberes tienen la obligación de respetar, proteger y**

satisfacer los derechos humanos, que constituyen la base legal para la reivindicación de derechos y la demanda de reparación en caso de incumplimiento"

Dentro de los principios que inspiran a los derechos humanos, está el de que estos son inalienables, característica que hace que ninguna persona pueda ser despojada de estos, excepto en situaciones legales claramente definidas; así mismo la obligación de proteger los mencionados derechos, exige a los países a tomar las previsiones, medidas u otros mecanismos de protección a fin de evitar que se cometan abusos tanto en la realidad como en la esfera virtual, por parte de agentes extragubernamentales u otros, buscando proteger, respetar, y cumplir con dichos derechos.

Es así que el tema bajo el que se centra el presente trabajo, la intimidad, se constituye como un Derecho Humano, el cual se circunscribe dentro de la esfera de derechos civiles y políticos. **(s/a, Derechos Humanos Manual para Parlamentarios, 2005, pág. 2)**

En nuestro país, el sumo intérprete de la Constitución Política, el Tribunal Constitucional, señala en una de sus jurisprudencias:

> *"**La dignidad humana constituye tanto un principio como un derecho fundamental; en tanto principio actúa a lo largo del proceso de aplicación y ejecución de las normas** por parte de los operadores constitucionales, y **como derecho fundamental se constituye en un ámbito de tutela y protección autónomo**, donde las posibilidades de los individuos se encuentran legitimados a exigir la intervención de los órganos jurisdiccionales para su protección ante las diversas formas de afectación de la dignidad humana (FJ 10)"* **(Tribunal Constitucional, 2006)**.

Reforzando lo anterior.

> "***La dignidad del ser humano es un principio fundamental (materialmente insuperable)** de contenido propio de la constitución material, por cuanto **es a través de él que el***

***sistema político define la situación de la persona en y frente al Estado y a la sociedad**, por tanto debe ser protegida y promovida en cuanto al derecho a la identidad, garantizando una vida digna (FJ 5 -7)"* **(Tribunal Constitucional B, 2006)**.

Así mismo:

"*El contenido esencial de un derecho fundamental no puede ser determinado a priori. Dicho contenido esencial es la concreción de las esenciales manifestaciones de los principios y valores que lo informan, su determinación requiere un análisis sistemático de este conjunto de bienes constitucionales, en el que adquiere participación medular el principio-derecho de dignidad humana, al que se reconducen, en última instancia, todos los derechos fundamentales de la persona (FJ 21)"* **(Tribunal Constitucional, 2005)**.

El Principio N° 10 de la Comisión Interamericana de Derechos Humanos señala: "Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o *persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público*".

(Álvarez Rodríguez, 2012, pág. 3) Señala respecto a la dignidad humana: "Se caracteriza por la dignidad humana como premisa antropológico-cultural, por la soberanía popular y la división de poderes, por los derechos fundamentales y la tolerancia, por la pluralidad de los partidos y la independencia de los tribunales (Haberle, 2003, p.3), ya que los mecanismos de defensa eran insuficientes para dar cabida a los valores superiores constitucionales".

En relación a lo dicho, toda persona humana, sin importar cualidades u otros atributos, cuenta con una dignidad que le confiere un valor superior y un lugar único en la sociedad, complementando lo

indicado "***La dignidad humana es un valor superior característico del estado constitucional, que constituye el fundamento de los derechos humanos*** considerados como el conjunto de facultades, prerrogativas y libertades que corresponde al hombre por el simple hecho de su existencia (Contreras, 2000, p. 5) por lo que deben ser reconocidos y garantizados por el Estado". **(Álvarez Rodríguez, 2012, pág. 3)**

> Actualmente la era de la información se convierte en la fuerza latente de la transformación social, capaz de acarrear una expansión en la calidad y en la cantidad de información y un aumento en gran escala del almacenamiento de la misma, las dos últimas décadas del segundo milenio marcaron un desarrollo incontenible del poder de la información, incluido el informático, se introdujo Internet, creando lo que hoy se conoce como ciberespacio. Puccinelli (2004, p.2) ***sostiene que es un marco virtual en permanente e incontenible expansión, en donde todos pueden participar aportando y recibiendo información, lo que implica, en el sentido positivo un inagotable dínamo de la libertad, sin embargo en su sentido negativo, es capaz de producir lesiones sobre los derechos fundamentales de los individuos***. **(Álvarez Rodríguez, 2012, pág. 2)**

La dignidad humana caracteriza a los derechos fundamentales donde el derecho a la intimidad protege un valor superior inherente a la persona, para establecer el vínculo que existe con el principio de autodeterminación informativa, que:

> [...] es un derecho cuya esencia radica en dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales (Lucas, 1990, p. 25); constituido también por la información personal y la vida privada, a partir de ahí en la tercera sección se establecerá el impacto que tienen las redes sociales en la actualidad y se planteará el derecho al olvido como una propuesta pertinente de la Unión Europea (ue) que pretende otorgar seguridad jurídica a los usuarios de internet; para concluir que ante la nueva realidad tecnológica se necesitan de mecanismos informáticos basados en pautas jurídicas que garanticen la autodeterminación informativa y la dignidad humana.
>
> **(Álvarez Rodríguez, 2012, pág. 2)**

i. Dignidad e inviolabilidad de la persona

Relacionando un poco el citado tema de la dignidad con la intimidad, se puede aludir a la ya desarrollada teoría de los derechos personalísimos, desde los cuales en la explicación siguiente se distinguirá el cómo confluyen los derechos que definen a la persona y le dotan de un valor inherente, tal es así, que la intimidad devendría en un rasgo de la dignidad humana, cuya integridad se constituye como parte de esa construcción denominada derechos personalísimos, veamos: "Engloba bajo ese título la referencia a varios de los derechos personalísimos tradicionalmente reunidos bajo el rótulo de "derechos de la integridad espiritual", y que de hecho se interrelacionan estrechamente: los derechos a la intimidad, al honor, a la imagen y a la identidad..." **(Navarro Floria, 2012)**

Otra acepción similar es señalada en la siguiente apostilla, cuyo tenor señala y refuerza lo establecido líneas arriba, enfatizando la relación entre la intimidad y la dignidad; "...***la persona tiene un valor en sí misma y como tal cabe reconocerle una dignidad***, de lo que se sigue que todo ser humano tiene frente a cualquier otro el derecho a ser respetado por él como persona, a no ser perjudicado en su existencia (vida, cuerpo, salud), y en su propia dignidad (honor, intimidad, imagen), y que cada individuo está obligado frente a cualquier otro de modo análogo. **(Rivera, 2012, pág. 151)**

Afectaciones a la dignidad

Este punto se examinará desde dos perspectivas: la enumeración de derechos tutelados y los efectos de la lesión a los mismos. En cuanto a los derechos tutelados por la dignidad puede señalarse que esta no es taxativa "*pues el texto comprende al menoscabo "de cualquier otro modo" de la "dignidad personal*"". **(Rivera, 2012, pág. 152)**

Por otro lado, trayendo a mención los efectos de lesionar la dignidad, se puede señalar: "... ***la persona que sufra una discriminación o se vea afectada en sus libertades podría ejercer las acciones tendientes a prevenir tal atentado o a obtener la reparación del daño que haya sufrido***" **(Rivera, 2012, pág. 152)**

Derecho al honor y a la identidad

Los derechos personalísimos reciben también protección del Derecho Penal, como por ejemplo ocurre con la tipificación de delitos contra el honor (calumnias, injurias, denuncia calumniosa) **(Navarro Floria, 2012)**

En cuanto al derecho a la identidad, comprende tanto la identidad biológica, la sexual y la identidad dinámica de acuerdo a los criterios que ha desarrollado la jurisprudencia italiana que tiene repercusión en la doctrina argentina. **(Rivera, 2012)**

La idea de que los derechos de la personalidad pueden disponerse y que el consentimiento para la disposición es libremente revocable tiene sólidos antecedentes en el derecho comparado ya que aparece por vez primera en el Código Civil de Portugal (art. 81) **(Rivera, 2012)**

Dignidad, intimidad e informática

Nuestra Constitución Política del Perú de 1993 en su artículo 2 inciso 6 establece lo siguiente:

"*Toda persona tiene derecho: a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar*".

"Sobre este artículo el señor Ferrero Costa hace una aclaración importante: Cuando se refiere a "los servicios informáticos", no se refiere a los servicios públicos y privados (como en algún medio de prensa se ha pensado), se refiere al uso de las computadoras para manejar la

información que sobre la sociedad y las personas existen". **(Basilio Araujo & Samamé Toribio, 2008, pág. 2)**

En ciudades enormemente informatizadas, el uso del dato personal es sumamente peligroso si es que no se establecen las garantías constitucionales del caso para proteger a las personas; por eso, las constituciones más modernas, como la última de Brasil, Colombia o concretamente Portugal, han establecido ya, y en otros casos leyes especiales, como en Estados Unidos, normas que protejan a las personas de los excesos que se pueden cometer a través de la informática, tanto el sector público como en el privado **(Basilio Araujo & Samamé Toribio, 2008, pág. 2)**

Así mismo "la información sobre una persona, es un derecho de la persona y por lo tanto hay que proteger a esas personas cuya dignidad hemos declarado que vamos a respetar y promover, hay que apoyarla para que pueda defenderse del mal uso de la informática **(Basilio Araujo & Samamé Toribio, 2008, pág. 2)**

¿Cómo exigir que los servicios privados acaten el precepto constitucional en favor del usuario de internet o persona humana?

Aludiendo directamente a la interrogantes antes planteadas, un parámetro a considerar es que la persona como entidad a la que le corresponden los derechos de por sí, "...***debe tener el derecho de conservar la información personalísima que tiene***, aquí obviamente habrá que hacer también alguna excepción, como en toda regla. Por eso se establece que salvo los casos de seguridad nacional que se establezcan por ley, o sea que solamente por ley puede establecerse, qué datos pueden ser considerados en los medios informáticos públicos y/o privados". **(Basilio Araujo & Samamé Toribio, 2008, pág. 3)**

Para llenar la deficiencia antes citada, existe una norma reciente cuya denominación es "Ley de protección de datos personales", sin embargo y luego de entrar en plena vigencia, se debe señalar que esta ley discrimina los servicios privados solo para las empresas que se encuentran en nuestro territorio, pero, qué hay de los que más hace uso la población y que no cumplen con el supuesto de ley antes expuesto, ¿porque otros países si pueden obligar a google, facebook entre otros a acatar su normativa? ¿Qué sucede en nuestro país? Es de esperar que la respuesta llegue casi instantáneamente "no es de competencia territorial" entonces todas las personas deben estar desamparadas por usar los servicios o aplicaciones de internet sin esperar que respeten en ninguna circunstancia sus derechos. Si una empresa de otro país maneja datos personales de personas extranjeras de otro país, porque no lo hace respetando la ciudadanía de ellas como se haría en un país ajeno al natal, es decir cuando esta un extranjero en otras tierras o aplicando su jurisdicción si adoptase la posición de una embajada.

En una sociedad informatizada que quiera respetar la dignidad de las personas, la regla tiene que ser precisamente interna, siguiendo los lineamientos de la Constitución. El principio es que, los datos personales tienen que ser de uso y manejo exclusivo de cada persona, con excepción lógicamente de lo que se establezca por razones de seguridad nacional. **(Basilio Araujo & Samamé Toribio, 2008, pág. 3)**

Acaso no constituye un asunto de seguridad nacional defender los datos personales (datos íntimos, sensibles) que muchas empresas extranjeras trafican de los ciudadanos que diariamente usan aplicaciones de Internet por necesidad, acorde a los lineamientos de los derechos humanos al establecer como una necesidad el libre acceso a la red.

Porque la legislación permite la despersonalización y la cosificación de la persona en internet, acaso perdemos nuestros derechos o

renunciamos a todos ellos cuando navegamos en internet y nos convertimos en objetos susceptibles de ser ofrecidos al mejor postor, dejamos nuestra condición humana y nos convertimos en simples datos.

B. Derechos de la personalidad y la intimidad

Históricamente estos derechos reconocen y protegen la naturaleza dela persona, como el derecho a la vida, la libertad, el honor, la intimidad, la privacidad y la imagen, fueron introducidos en la doctrina universal en siglo XIX **(Wikipedia (C), 2014)**, produciendo un reconocimiento aislado, germinal y primigenio hasta el siglo XX donde fueron reconocidos por la Declaración Universal de los Derechos Humanos en 1948 o el Pacto de San José de Costa Rica (1969).

En nuestra normativa, se sabe y es un hecho jurídico que toda norma se centra en la persona, la cual se caracteriza por ser eminentemente social, pues para desarrollarse necesita de una comunidad, relacionándose con sus semejantes y desarrollando toda una serie de actos que hoy son connotados como jurídicos, de esta forma hoy todos somos particulares en nuestro modo de ser y cada uno posee una personalidad singular, dicho esto, existe un tipo de derechos esenciales para la persona, que son definidos como derechos de la Personalidad o derechos personalísimos, así **(Machicado, 2012)** plantea: "**Los Derechos de la Personalidad son una categoría especial de los Derechos Humanos, cimientos jurídicos, estos, que están en la Declaración De Los Derechos Del Hombre Y Del Ciudadano del 26 agosto 1789 texto fundamental en virtud del cual se definen los derechos "naturales e imprescriptibles**" continuando con lo anteriormente señalado, **(Gutiérrez David, 2013)** expresa: "los denominados derechos de la personalidad o personalísimos, entre los que tradicionalmente **se incluyen el honor, la intimidad y la vida privada y la propia imagen**", así mismo **(Machicado, 2012)** añade: "**Los derechos de la personalidad son bienes jurídicos**

que se caracterizan por ser privados, absolutos, extra- patrimoniales y que el ser humano no necesita adquirirlos salvo casos excepcionales".

Señala **(Herrán Ortiz, 2003, pág. 10)** "**la intimidad es un derecho de la personalidad porque constituye un bien instrumental para garantizar la libertad del individuo en el desarrollo de su propia vida**." Este precepto humano se ve reforzado por **(Herrán Ortiz, 2003, pág. 10)** "**el derecho a la intimidad se configura como elemento esencial para el desarrollo de la personalidad**"

Sin embargo, donde encajan los derechos humanos y en qué posición se encuentran, si los derechos de personalidad son tan primordiales, al respecto explica **(Machicado, 2012)** la distinción entre derechos humanos y los derechos de personalidad que se están tratando: "**Los Derechos Humanos son de carácter público cuya base está en la Constitución política del Estado. Los Derechos De La Personalidad son de carácter privado inmerso el Derecho Civil porque todos los derechos subjetivos que reconoce la Constitución política del Estado son reconocimiento a los Derechos Humanos**", de este modo se dilucida y se caracteriza los derechos de personalidad con los derechos humanos.

Definiendo los derechos de personalidad a continuación se presenta una serie de conceptos:

- JERKE dice que son derechos que garantizan a toda persona el señorío sobre una parte de sus derechos esenciales.
- FERRARA: Derechos que protege al ser humano y constituye la manifestación de sus facultades físicas espirituales.
- DE CASTRO: Derechos que garantizan al sujeto la protección y tutela de sus bienes jurídicos más esenciales.

- DOMENICO BARBERO: **Derechos subjetivos absolutos privados extra-patrimoniales que posee toda persona por ser tal y que garantizan la tutela y protección de los bienes jurídicos inmersos en el ser humano** como ser la vida, la integridad física, el nombre, el domicilio, la correspondencia, etc. **(Machicado, 2012)**

De los conceptos señalados, el que mejor reúne las características de los derechos de personalidad es el último, pues dota de subjetividad al derecho, le confiere el rango de absoluto, discrimina su naturaleza privada, la cual no es un bien patrimonial, que en suma garantiza diferentes aspectos que hacen a la persona y la definen, una de esas características es la intimidad.

En cuanto a la denominación del sobre el derecho a la personalidad, se puede mencionar que se le conoce como "derecho esencial, derecho innato, derechos privados del sujeto, derechos personalísimos y como ya se ha señalado bastante, derecho de la personalidad"

Para establecer cuál es el objeto de aplicación de este derecho a la personalidad señala **(Machicado, 2012)**, "se decía que **el objeto de los derechos de la personalidad está en la persona**, en el cuerpo humano. **Nicolás Cobieno dice que nadie puede ser a la misma vez objeto y sujeto**. Para rebatir dicen que los derechos de la personalidad son derechos sin sujeto. Pero no es científico aceptar derechos sin sujeto." Explicando con más detalle y resolviendo la cuestión anterior, **(Machicado, 2012)** señala: "**La Escuela Latinoamericana entonces señala y distingue que el sujeto es la persona como unidad física y moral en forma completa como titular de derechos y deberes. El ser humano es persona porque la ley así lo reconoce.**"

En cuanto a la naturaleza o fundamento de los derechos de personalidad "Iuris et de iure"[9] se puede establecer que son patrimonios jurídicos inherentes a la persona como tal, de este modo como se dijo anteriormente en las denominaciones, estos derechos son consustanciales a la naturaleza del hombre, en tal sentido son instrumentos jurídicos, inmersos dentro del ordenamiento positivo, constituyendo derechos plenamente subjetivos, de los cuales la persona puede hacer valer en cualquier momento cuando se manifieste una vulneración por un tercero, mientras tanto estos derechos son parte de la persona y no una condición prestada por la ley, los cual sirve para exigir a terceros una conducta acorde a los lineamientos legales pertinentes en ambos sentidos, es decir de persona a persona.

En cuanto a las características de los derechos a la personalidad presenta tenemos:

- ORIGINARIOS E INNATOS.- Porque son derechos que nacen con la persona y no se la adquiere, excepto en la correspondencia epistolar que se crea mediante acto.
- ABSOLUTOS.- Porque son oponibles a todo el mundo ("erga ommes"[10]) que está obligado a no desconocer los Derechos De La Personalidad. Es que el ser humano en razón de que son derechos subjetivos tiene la facultad de actuar sobre los mismos en forma exclusiva con prescindencia de los demás, nadie vive por otro.
- PRIVADOS.- Porque están en la esfera del derecho Civil y su vulneración da lugar a la indemnización. Aunque puede ser derechos subjetivos de carácter público cuando revisten caracteres de Derechos Humanos.
- EXTRAPATRIMONIALES.- Porque están fuera del comercio humano excepto los autorizados por ley, por ejemplo la explotación de la imagen.

---

[9] *Locución latina: De pleno y absoluto derecho*

[10] *Locución latina. Contra todos o respecto de todos. Se emplea jurídicamente para calificar aquellos derechos cuyos efectos se producen con relación a todos, y se diferencian de los que sólo afectan a persona o personas determinadas.*

- INDISPONIBLES.- Porque son de orden público, es decir la voluntad de la persona no puede crearlos, modificarlos, reglamentarlos, transmitirlos ni extinguirlos:
  - NO SE CREAN, porque son innatos, excepto los permitidos por ley: el pseudónimo, la correspondencia epistolar.
  - INTRANSMISIBLES, porque son "res extra-comercium" excepto en donaciones altruistas de órganos del cuerpo.
  - INMODIFICABLES, porque no dependen de la voluntad, excepto en el nombre.
  - IRRENUNCIABLES, porque nadie puede autorizar a ser denigrado.
  - IMPRESCRIPTIBLES, porque no se puede adquirir por usucapión, no perder por prescripción extintiva o liberatoria. **(Machicado, 2012)**

C. La Intimidad y sus tipos de vulneración

Rescatando lo expresado en la página **(Webjurídico, s/f)** donde se realiza una taxonomía de las situaciones y lugares donde se produciría una violación al derecho a la Intimidad veamos el primero referente al domicilio: "***es el espacio vital donde cada persona desarrolla su vida privada a través de la intimidad además del derecho de propiedad exclusivo de todo domicilio***." **(Webjurídico, s/f)**

Haciendo un pequeño análisis de lo visto en las líneas precedentes, se podría afirmar que un correo electrónico o una cuenta de internet, comparten similares atributos a los del domicilio, pues en cada uno de los mencionados se desarrolla de alguna manera y en algún grado la vida privada de cada persona y cada uno de los datos creados en dichas plataformas constituirían un patrimonio o propiedad exclusiva e inherente a la persona como usuario.

Siguiendo con el orden de ideas, **(Webjurídico, s/f)** señala en concordancia, una segunda característica en donde se producirían violaciones al derecho a la intimidad, el cual concierne al derecho al

secreto, como explica: "al tener una vida privada implica a todo individuo a resguardar determinados datos del conocimiento público ya que si estos fueran divulgados supondría una violación de la intimidad de todo sujeto, **ya que si se deposita en otras personas la confianza de ciertas cosas, estas deben de seguir siendo secreto y no ser publicadas**"

Desarrollando la idea anterior, esta situación no estará ocurriendo en las cuentas de internet, ya que se confía en determinadas aplicaciones datos personales y sensibles "íntimos" que de acuerdo a la naturaleza de cada quien, es susceptible de compartir en alguna forma o no, sin embargo ello no significa que otros hagan usos inapropiados de dicha información solo por el hecho de poseerla.

Descomponiendo lo presentado, señala **(Webjurídico, s/f)** "**La diferencia entre el secreto y la intimidad es aquella en que el depositario del secreto no es titular de un derecho de protección sobre el mismo ya que dicho secreto no afecta a su esfera privada**, siendo el depositario del secreto el que vería lesionada su intimidad si el mismo se divulgara y expusiera a la vista de otras personas por lo que el depositario tiene la obligación de guardar el secreto que se le haya confiado."

Un tercer punto que concierne a la protección a la Intimidad sucede en las comunicaciones, a lo que **(Webjurídico, s/f)** anota: "**a través de ella se pueden exteriorizar sentimientos, ideas y tendencias, por medio de gestos, escrituras, o por medio de la voz**. Toda intromisión en las mismas extraña una violación del secreto de la comunicación"

Del punto bajo análisis se puede señalar que a la intimidad no se le brinda la protección debida, pues de que todo lo que creamos y exteriorizamos en Internet, en diversas aplicaciones, en buena cuenta se le resta el aspecto de la propiedad como un bien que se debe proteger en

favor de la persona, toda esa información creada, comunicada, exteriorizada surge de la intimidad, en que parte de nuestra legislación se le confiere además de un estatus intimo a estas comunicaciones que hacemos por diferentes canales en Internet, la protección debida, por otro lado, lo propuesto solo es una parte de lo que en realidad representa, pues **al escribir manifestamos, nuestras creencias, tendencias y hasta nuestra personalidad**, así lo demuestra la **(Universidad de Cambridge, 2015)** que en convenio con Facebook han ideado una aplicación *("You are what you like"*), la cual puede desentrañar nuestra personalidad previa aceptación, para que acceda a los datos de nuestra cuenta y la analice, esto es solo un indicador de los datos que maneja esta red social, pero, la intimidad en otras aplicaciones y en el mismo Facebook, al dar tratamiento a estos y otros datos donde queda.

En cuarto lugar, tenemos lo concerniente al secreto de los documentos, para lo cual, **(Webjurídico, s/f)** señala "Los documentos al igual que el resto de las comunicaciones **han de ser preservadas de destinatarios que no son los propios de la condición de la comunicación entre destinatarios**, por eso han de ser igualmente protegidas contra cualquier injerencia que pueda producir daños tanto al remitente como al destinatario."

Otra arista que se explica de la intimidad y son las aplicaciones en las que confiamos nuestros datos, secretos u otros, pero nos comunican si existe alguna intromisión a nuestra cuenta para que como titulares del derecho accionemos algún medio de defensa en particular o por lo menos nos demos por enterados, en qué sentido se efectiviza la garantía proclamada por la constitución y resguardada por el habeas data si somos sujetos de espionaje o monitorización de nuestras comunicaciones por parte de entidades u organismos gubernamentales fuera del territorio nacional, alcanzará dicho proceso constitucional para defender mis intereses. De otro lado existe una protección penal que se encarga de

actos ilícitos como el hackeo de las comunicaciones, sin embargo, ***que medio existe para resarcir el daño causado por la injerencia de un delito en la intimidad de los ciudadanos***.

Una quinta forma de vulneración a la intimidad surge del secreto profesional, pero al llevarlo al contexto que explicamos, como puede existir el secreto profesional en la red conocida como internet, antes de tentar una posible relación o nexo veamos los que **(Webjurídico, s/f)** dice en relación al secreto profesional: "**Algunos profesionales tienen el deber moral o jurídico de no revelar ciertos datos dados por el cliente**, ya que tiene su fundamento en la defensa de la intimidad del depositante del secreto que a determinados profesionales,"

Como entonces nos envían ofertas si no han desvelado nuestros intereses, se habrá creado algún nuevo tipo de secreto con las empresas prestadoras de aplicaciones en internet, la respuesta es aparentemente obvia, ***donde queda el deber de los ingenieros de software, sistemas, etc. al crear una aplicación que resguarde la intimidad desde su diseño***.

Por último y quizá el más conocido y el que más tratamiento a nivel legislativo ha merecido, es el empleo de tratamiento informatizado de datos veamos:

> "*En la actualidad recibimos a menudo en nuestros buzones propagandas de lugares o locales en los que no hemos estado nunca o propaganda de entidades que se dedican al marketing, situaciones que ponen en riesgo la intimidad.* ***Por eso es necesario que se protejan esas bases de datos y todas aquellas informaciones de carácter personal que tienen las empresas que se dedican a vender estos datos***. *El atentado contra la intimidad por el uso de la informática puede provenir tanto de la recogida de datos como aquellos que pueden afectar a la esfera más personal. ...Los afectados tienen derecho a ser informados previamente a la recogida de datos para constituir el fichero.* **(Webjurídico, s/f)**"

Nuestra legislación considera legalmente el tema del "spam", para lo cual ha creado una ley en particular que regula aspectos relativos a este, sin embargo, la situación del Spam y la intimidad no se ha interpretado debidamente en los correos u otras cuentas electrónicas, donde se revisan todas las comunicaciones para que en base a un tratamiento automatizado se pueda ofrecer una determinada publicidad en base a las preferencias (eso no es introducirse en la esfera íntima de cada persona), donde aparte de servirse de nuestra experiencia en el uso de su aplicación en pro de su mejora sacan aún más provecho de nuestro "hacer" para leer toda la información que generemos y nos ofrezcan propaganda en base a ese análisis que dicho sea de paso vulnera aún más nuestra esfera íntima, y aun así creemos que dichas aplicaciones son gratuitas.

Se debe informar previamente de la recogida de datos solamente, se puede fácilmente llenar este vacío al momento de aceptar el acuerdo de las condiciones de servicio, para lo cual se entenderá que se ha informado que sus datos serán procesados, lo que no se ha dicho es cuando, donde y quien lo hace, ni de qué parte de la información, además de que sirve lo dicho, si dichos términos y condiciones de servicio cambian fácilmente y en la forma en que más le parezca al que ofrece su aplicación en internet, **que norma nos brinda estabilidad contractual para dichas aplicaciones**, debiere al momento de cambiar dichos términos de servicio de obligarse a la empresas digitales de devolver todos los datos que hasta ese momento poseen de dicha persona y como se dice comenzar de cero, para que este cambio pueda apreciarse en las empresas que prestan sus aplicaciones y no tomen tan a la ligera los contratos que tan sutilmente cambian y la forma y el momento que mejor les parece y les conviene.

Como parte de este último considerando **(Webjurídico, s/f)**, hace un complemento informativo, "***Se tiene derecho por parte del responsable del fichero en caso de que se produzca una lesión en sus bienes o derechos debiendo indemnizar al que los ha sufrido." "Lo mismo ocurre con los ficheros de informática y el peligro que conllevan ya que se manipulan informaciones y lo peor es que son desveladas con toda impunidad.***"

Tomando en cuenta la "Ley de protección de Datos", no ha previsto ni siquiera remotamente la teoría del daño causado a los usuarios de internet por la responsabilidad de las empresas que son depositarias de informaciones que solo les competen como titular a los usuarios, como se podría resarcir un daño que ni siquiera se toma en cuenta.

2.2.3 BASES CONSTITUCIONALES Y CONCEPTUALES

A. Derechos constitucionales de aplicación a la intimidad y los datos personales

Derecho fundamental

Al abordar esta temática conviene definir qué son los derechos fundamentales en principio y cuál es la relación que guardan con las personas en razón a su contenido, esencia y justificación, en tal sentido una definición acorde a lo señalado la plantea Miguel Carbonell:

> "*los derechos fundamentales son considerados como tales en la medida en que constituyen instrumentos de protección de los intereses más importantes de las personas, puesto que preservan los bienes básicos necesarios para poder desarrollar cualquier plan de vida de manera digna; siguiendo a Ernesto Garzón Valdés podemos entender por bienes básicos aquellos que son condición necesaria para la realización de cualquier plan de vida, es decir, para la actuación del individuo como agente moral*". **(Carbonell, 2004, pág. 7)**

Desde la teoría del derecho como enfoque de estudio y análisis de los derechos fundamentales, debe contar con características que se establecen en la definición teórica del derecho **(Carbonell, 2004, pág. 6)**, para que un derecho sea fundamental desde la perspectiva de análisis dogmático, este debe contar con una justificación y fundamento jurídico, es decir cuando un texto constitucional reconoce ese derecho **(Carbonell, 2004, pág. 6)** , por ultimo desde la perspectiva sociológica o historiográfica un derecho fundamental encuentra su justificación en la medida en que se haya realizado en la práctica o en la connotación histórica que haya tenido, es decir que no haya sido pura idea de algún pensador sino que haya obtenido alguna repercusión en la práctica **(Carbonell, 2004, pág. 6)**.

i. Protección a la Intimidad por la Constitución Política

El constitucionalista Enrique Bernales Ballesteros señala:

> "No obstante la prohibición de estas limitaciones, la Constitución dice que los derechos se ejercen "bajo las responsabilidades de ley". Estas responsabilidades pueden ser tanto administrativas (por ejemplo multas), como civiles (indemnizaciones por daño causado) y penales (penas de diversa naturaleza), en concordancia con los tipos de sanciones previstos en la legislación. Pero que sanción hay para los ejercen estas limitaciones o vulneraciones en la red Internet, fuera de nuestro país. **(Bernales Ballesteros, 1999, pág. 120)**

Artículo 2.- Toda persona tiene derecho:

En el inc. 5 del referido artículo de nuestra Constitución refiere:

"*A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga este pedido.* ***Se exceptúan las informaciones que afectan la***

intimidad personal *y las que expresamente se excluyan por ley o por razones de seguridad nacional*".

Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

Siguiendo con la explicación, señala **(Bernales Ballesteros, 1999, págs. 122-123)** *"La información del Estado es información de todos y no puede ser restringida. Los límites son el derecho a la intimidad personal, que también es de jerarquía constitucional (artículo 2 inciso 7) y la información clasificada como reservada para fines de seguridad nacional"*

La protección del mencionado artículo debe extrapolarse con el Art. 200 referido a las garantías constitucionales, específicamente con el Hábeas Data. "Como se sabe, esta es una garantía novedosa de la Constitución, tomada de la experiencia brasileña, que puede interponerse cuando se vulnera o amenaza los derechos a que se refiere el art. 2, incisos 5 y 6 de la Constitución" **(Bernales Ballesteros, 1999, pág. 123)**.

Inc. 6. "*A que los servicios informáticos, computarizados o no, públicos o privados,* ***no suministren informaciones que afecten la intimidad personal y familiar***".

El Inc. 6. Refiere un punto muy importante para el presente trabajo investigativo, pues señala un principio constitucional esencial, debido a que frecuentemente se vulnera este precepto y no existe un medio económicamente razonable para ejercer una acción legal para protegerlo.

El constitucionalista explica:

> "Esta es una forma de protección de la intimidad que se traduce en la prohibición de divulgar información sobre las personas y las familias... (..) ... **Por servicio informático debemos entender, extensivamente -pues la fórmula que emplea el texto**

constitucional es confusa-, todo sistema de archivo de información sobre el ámbito personal y familiar. La información puede cubrir los aspectos más diversos de la vida: características personales (incluidas las historias clínicas, por ejemplo), habilidades personales (registros de notas en materia de educación en general), capacidades laborales (hojas de servicios, pruebas de calificación laboral, etc), registros de vida (archivos policiales, de inteligencia o similares). La norma constitucional no se restringe sólo a este tipo de información. Al contrario, su espíritu es referirse a toda aquella que de una u otra manera afecte la intimidad de la persona o su familia. **(Bernales Ballesteros, 1999, pág. 124)**

Un análisis extensivo del inciso se puede apreciar más adelante:

"Entendemos que la norma no se refiere sólo a los archivos de información computarizados, sino a todos los que contengan información, al margen de la tecnología de acopio y registro que utilicen. Este enfoque supera el error de formulación en que incurrieron los constituyentes al emplear el término "servicios informáticos", en lugar de "servicios de información". La informática, según los alcances aceptados por el Diccionario de la Lengua Española, es el "conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático de la información por medio de calculadoras electrónicas". Así pues, no puede haber un "servicio informático" que no esté computarizado, como equivocadamente dice a la letra el inciso bajo comentario. Pero este error de los constituyentes queda superado al interpretarse extensivamente que se trata de una manera más amplia y general de servicios de información, computarizados o no. En todo caso, una reforma de la Constitución debería modificar el texto e introducir la expresión correcta: servicios de información. **Se evitarían así confusiones y restricciones de este derecho**". **(Bernales Ballesteros, 1999, pág. 125)**

Corrobora lo anteriormente dicho y en extensión del mismo inciso señala: **(Bernales Ballesteros, 1999, pág. 125)** "La prohibición de divulgar la información se extiende a los servicios de información privados o del Estado porque ***la violación de la intimidad no es realizada sólo por quien tiene autoridad, sino por todo aquel que divulga información***. Además, en el mundo moderno, muchas veces los archivos

privados de información pueden ser de calidad e intensidad igual o superior a los archivos públicos."

El Inc. 7 de nuestra constitución establece:

"*Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias*".

Analizando el presente inciso del artículo segundo de la constitución, puede disgregarse cinco derechos que aunque son distintos tienen una base común asentada en los derechos de la personalidad, y la dignidad de la persona, al respecto **(Bernales Ballesteros, 1999, pág. 125)** refiere en primer lugar: "El honor es el sentimiento de autoestima, es decir, la apreciación positiva que la persona hace de sí misma y de su actuación. El honor es violentado cuando esa autoestima es agraviada por terceros. Tales los casos de una ofensa -en público o en privado-, o de una agresión física, psicológica o espiritual. En este sentido, ***el honor es un sentimiento eminentemente subjetivo que, sin embargo, es susceptible de ser objetivamente defendido por el Derecho***".

En cuanto al segundo derecho que puede disgregarse del inciso bajo estudio es "la reputación", **(Bernales Ballesteros, 1999, pág. 126)** amplía: "La reputación es la idea que los demás tienen o presuponen de una persona. Es la imagen que los demás tienen de cada uno nosotros como seres humanos. La reputación es agraviada cuando nuestra imagen en los demás es dañada. Importante es decir que el daño a la reputación es producido tanto cuando se dicen mentiras, como cuando se dicen verdades dañosas. No es menos atentatorio contra el derecho a la reputación el imputar públicamente algún defecto o alguna condición negativa que tenga determinada persona".

Respecto a lo mencionado anteriormente, existe una incidencia relativa en este sentido, cuando se imputa sin prueba suficiente, el haber

cometido una infracción contra los derechos de autor o incumplido con términos y condiciones de servicio de alguna aplicación en Internet y se prive el acceso a una cuenta de correo por ejemplo, o alguna información electrónica, sin la posibilidad de accionar una defensa, o el pedido de cancelación de los datos referidos al usuario de Internet o usuario virtual.

En contraste a lo señalado de los derechos al Honor y la reputación, **(Bernales Ballesteros, 1999, pág. 126)** agrega: "son derechos complementarios de la persona, pues se refieren a su estimación desde dos perspectivas confluyentes: la de ella misma y la de los terceros para con ella.

En cuanto al tercer derecho que se disgrega del inc. 7 del Art. 2 de la constitución, encontramos a la intimidad al respecto **(Bernales Ballesteros, 1999, pág. 126)** expresa: "**La intimidad es el conjunto de hechos y situaciones de la vida propia que pertenecen al ser humano como una reserva no divulgable**. Entre otros están sus ***hábitos privados, sus preferencias, sus relaciones humanas, sus emociones, sus sentimientos, sus secretos, sus características físicas*** tales como su salud, sus problemas congénitos, sus accidentes y las secuelas consiguientes, etc".

Al emprender un análisis de la intimidad de acuerdo a lo establecido por el inc. 7, se puede descomponer en dos dimensiones veamos:

> ***La Constitución da dos dimensiones a la intimidad que, en realidad, son complementarias: la personal y la familiar***. La intimidad personal *es el ámbito restringido en torno al individuo mismo. Es aquella intimidad que, incluso, puede negarla a sus familiares*. La intimidad familiar *son todos los eventos y situaciones que pertenecen a las relaciones que existen dentro de la familia: las relaciones conyugales, de padres e hijos, de hermanos, etc*. Es lógico que la intimidad asuma estas dos dimensiones y particularmente la última, en la medida que la familia es una unidad

natural de socialización del ser humano, con alto contenido emocional y sentimental, dentro de la cual se producen situaciones y relaciones de incomparable intensidad en relación a las que cada persona pueda tener con terceros. Por ello mismo, ***es un ámbito reservado a las invasiones externas***. **(Bernales Ballesteros, 1999, pág. 126)**

Llegando a la cuarta cualidad jurídica o cuarto derecho al que hace referencia el inciso bajo estudio, encontramos el derecho a la "propia voz" que consiste en aquella cualidad que únicamente pertenece a la persona, ampliando **(Bernales Ballesteros, 1999, pág. 127)** explica: "El derecho a la propia voz -aspecto que no consideró la Constitución de 1979- consiste en que la utilización por parte de una persona de su voz sólo puede hacerla ella misma o aquel a quien autorice; en ese contexto, la voz es parte de uno mismo y de la identificación personal. ***En realidad es como el cuerpo, la cara y, también, como la manera propia de pensar***".

Por último encontramos el derecho a "*la propia imagen*", **(Bernales Ballesteros, 1999, pág. 127)** señala: "El derecho a la propia imagen consiste en que la representación corporal de una persona sólo puede ser utilizada por ella y por aquellos a quienes autoriza. El derecho tiene que ver con la representación corporal que es la imagen captada en el cine, la televisión o el video, pero también la imitación y, aún, la caricatura. ***La propia imagen es protegida porque identifica al titular como ser humano***; consecuentemente, éste tiene el derecho de prohibir su reproducción".

En resumen tenemos:

"***En materia de todos estos derechos estamos hablando de las dimensiones privadas de las personas, porque cuando alguien tiene una responsabilidad pública y actúa en ejercicio de dicha responsabilidad, entonces la protección de estos derechos requiere matices: siempre estará protegida la privacidad de la persona***, no importa qué responsabilidad ostente, pero su imagen, su voz y los hechos importantes que se refieran a

su gestión pública, o que perteneciendo a su esfera privada influyan en la pública (por ejemplo, un alto magistrado del Estado que sufriera deterioro mental significativo) sí pueden ser utilizados públicamente, desde luego, guardando el debido respeto por la persona. En esto, como resulta obvio, hay límites que en ciertas circunstancias son muy difíciles de trazar. En los casos límite, tendremos que adecuarnos a los dos principios que guían la actuación pública de las personas: respeto a la privacidad pero información sobre los aspectos de su vida pública o que perteneciendo a la privada influyan decisivamente sobre aquélla. **(Bernales Ballesteros, 1999, págs. 127-128)**

En aporte a lo antes señalado podemos señalar:

"Para que se cumplan debidamente los supuestos de la norma, la afectación o el agravio a la persona tienen que producirse por las afirmaciones realizadas en cualquier medio de comunicación social. Los medios de comunicación social son la prensa escrita, hablada y televisada. Recientemente, sin embargo, pueden considerarse como medios de comunicación social las redes telemáticas, en las cuales puede diseminarse información a millones de personas en todos los países del mundo, con muy poco esfuerzo y costo (por ejemplo, a través de Internet). **(Bernales Ballesteros, 1999, pág. 128)**

Para nuestros tiempos donde la red conocida como internet ha cobrado especial y determinante importancia en la relaciones sociales, el inciso bajo comentario del art 2, tiene necesidad de una ley que regule sus alcances principalmente en las aplicaciones de Internet, es más, nuestra legislación debe crear mayores garantías para defender nuestros derechos, por hacer un ejemplo nuestro país debe hacer que las aplicaciones de internet respeten las normas referentes a los usuarios peruanos que acceden a determinada aplicación de gran relevancia social, solicitando que se pueda rectificar, cancelar o solicitar el derecho al olvido en determinadas circunstancias, de otro lado, hacer más asequible a todos el poder solicitar una defensa a nuestros derechos de forma simplificada a través de un proceso administrativo u otro de bajo costo y de fácil manejo.

Está bien usar un servicio bajo determinadas condiciones pero no por eso la información que situamos en dicho servicio deja de pertenecernos, es de alguna forma parte de nuestra creación intelectual, ya que como se dijo anteriormente hasta nuestra manera de pensar constituye una de las características que definen a la Intimidad, visto de esta forma, dichas empresas prestadoras de servicios digitales, nos niegan la posibilidad de reclamar derechos, frente a nuestras creaciones intelectuales e informaciones privadas, que en sus bases de datos se ubican, colisionando de manera indirecta y complementaria con la interpretación del Art. 2 Inc. 7 y 8 indirectamente.

Al respecto la doctrina señala:

> "En un sentido más amplio, la libertad de creación debe concordarse con otros derechos constitucionales, como la libertad de conciencia, la libertad de expresión, el derecho a la cultura y el libre desenvolvimiento de la personalidad, la información creada es fruto de la inteligencia humana, se podría hasta decir que es parte del desarrollo de las ideas filosóficas de cada persona donde esta [La protección moral a la creación, que consiste en el derecho a ser reconocido como el creador de la idea el escritor tiene derecho a que se diga que es el autor del libro, y si una persona decide publicar sus ideas y experiencia que tuvo a través de las redes sociales (es dueño también la empresa prestadora del servicio digital en la red)" **(Bernales Ballesteros, 1999, pág. 131)**

En último orden de análisis de las garantías constitucionales que tienen relación con la intimidad, ubicamos al Inc. 10 del art. 2 de nuestra constitución que establece:

"*Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados*".

En la tratativa del inciso mencionado el constitucionalista **(Bernales Ballesteros, 1999, pág. 137)** presta los siguientes alcances: "Las comunicaciones, telecomunicaciones o sus instrumentos ***sólo pueden***

ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los documentos privados obtenidos con violación de este precepto no tienen efecto legal".

La realidad expresa con acento discordante, que nuestra legislación no cuenta con medidas que eviten la intervención de otros Estados, organizaciones u otros, que intercepten las comunicaciones con diversos fines y diversos medios, sin que medien garantías al respecto con las que mínimamente podamos ejercer ante invasiones externas.

Respecto a las garantías constitucionales en sí, para proteger los derechos fundamentales, que para este caso en particular sería el hábeas data, donde el abogado **(Ortiz Gaspar, 2012, pág. 1)** hace referencia a una crítica en contraposición al carácter garantista del hábeas data: "Existe un cuestionamiento respecto a la utilidad del hábeas data e incluso algunos manifiestan su rechazo, por ejemplo Francisco Eguiguren señaló que "su existencia como proceso constitucional carece de suficiente justificación" y Samuel Abad comentó que "resulta innecesaria su incorporación en la nueva Constitución, pues para proteger este derecho bastaba con regular adecuadamente al proceso de amparo"."

En cuanto al derecho de rectificación que se mencionó, **(Bernales Ballesteros, 1999, pág. 130)** señala: "Ejercer la rectificación mediante carta notarial al director del órgano de comunicación, o acudir a la Acción de Amparo. Este extremo también es innecesario, pues la propia Constitución establece el Amparo para hacer valer determinados derechos, entre ellos, el de rectificación".

ii. Contenido del derecho a la intimidad en la constitución

Haciendo un pequeño reporte conceptual de lo que implica la privacidad remontémonos a la Constitución Política del Perú, como documento base y del que se disgregan todas las normas de nuestra legislación, en dicho sentido, **(La Constitución Comentada, 2005, pág. 57)**, "El derecho a la identidad que, como los demás derechos de la persona, se fundamenta en su inherente dignidad, posee su propia autonomía conceptual. Esta lo distingue de otros derechos que le son afines como los signos distintivos, el nombre o el seudónimo, **la intimidad de la vida privada, el honor, la reputación y el derecho personal del autor**."

De otro lado, la protección del derecho a la Intimidad, constituye un deber del Estado en palabras de **(La Constitución Comentada, 2005, pág. 71)**, "respetar la vida, la libertad, la integridad psicosomática, **la intimidad y el honor de los seres humanos**", esto significa que no solo se trata de un derecho inherente a la persona sino que se constituye en un deber del Estado el proteger este derecho sustancial de la persona.

El art. 5 de la constitución ya da atisbos de los derechos que vendría a protegerse, dentro de los que se considera intimidad de las personas, así detalla y explica nuestra constitución, Art. 5: A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. **Se exceptúan las informaciones que afectan la intimidad personal** y las que expresamente se excluyan por ley o por razones de seguridad nacional."

"Indagar sobre el derecho a la intimidad supone establecer una frontera entre aquello que debe permanecer reservado a la persona –lo privado– y aquello otro que quedará sometido al conocimiento y crítica de los demás –lo público–. En todo caso hacerlo, esto es reubicar los límites

entre ambos espacios, responde a una actual e inexcusable necesidad" **(González Cifuentes, 2011)**.

Al respecto se proponen tres formas de presentar el derecho a la intimidad

- Derecho a no ser molestado
- Derecho a ser desconocido
- Derecho a autopresentarse ante los demás **(González Cifuentes, 2011)**

iii. El derecho fundamental a la protección de datos personales

En la actualidad gracias a la tecnología, es posible acceder a casi todos los aspectos de la vida de las personas y, lo que es más importante, a través de técnicas novedosas (*data mining*) reconstruirla a partir de datos aparentemente inofensivos o carentes de interés, pudiéndose tomar decisiones basadas en los mismos.

La información citada en líneas anteriores, concuerda con lo expresado por **(Zaballos Pulido, 2013, pág. 55)** "Todo ello pone en manos del número creciente de personas, organizaciones y Estados, con acceso a los medios necesarios, un poder de control sobre los titulares de los datos que afecta directamente a su libertad, identidad y dignidad".

En nuestro contexto se ha desarrollado y normado los datos personales mediante el sustento del Art. 2 Inc. 6 de la Constitución Política del Perú en la Ley Nº 29733, Ley de Protección de Datos Personales (LPDP), que define al titular de los datos personales como la persona natural a quien corresponden los datos personales. La situación expuesta se desenvuelve en todo contexto tal es así que en España, se ha normado a través de la ley de protección de datos, al respecto **(Zaballos Pulido, 2013, pág. 55)** detalla: "la formulación del derecho a la protección de datos tiene su soporte en la Constitución Española de 1978,

ha sido la jurisprudencia del Tribunal Constitucional la que ha dado carta de naturaleza al mismo".

Agregando a lo señalado, se puede expresar que la esencia de dicha norma se halla en la constitución y en la necesidad de proteger datos íntimos de la persona como una necesidad social, al respecto acota **(Zaballos Pulido, 2013, pág. 55)** "Esta calificación tiene una gran importancia, ya que ***implica el reconocimiento de que estamos ante una exigencia esencial de la sociedad y la puesta a disposición de los titulares de los datos del mayor nivel de protección que el ordenamiento jurídico puede ofrecer*** así como de los instrumentos de tutela más poderosos".

Fundamentos de la protección de datos

Se presenta a continuación los fundamentos por lo que se debe proteger tan acuciosamente los datos personales, tan valiosos para los usuarios de Internet, **(Brian Nougrères, 2012, pág. 7)** comenta: "analizaremos las buenas prácticas en materia de protección de datos en la versión del Grupo de Trabajo de Comisionados Internacionales de Protección de Datos (2006)".

Los fundamentos de la protección de datos se pueden apreciar en:

A. Consentimiento

B. Rendición de cuentas

C. Finalidad

D. Limitaciones en la recolección

E. Limitaciones en el uso, la retención y la divulgación

F. Precisión

G. Seguridad

H. Apertura

I. Acceso

J. Cumplimiento

A. Consentimiento. Para el acopio, el uso y la exposición de la información personal es necesario que se recabe el consentimiento libre y específico del titular del dato. De este principio general solo se exceptúan aquellos casos que la ley indica. Cuanto más sensible es el dato, el consentimiento requerido deberá ser más claro y más específico. El consentimiento puede ser revocado.

B. Rendición de cuentas. Toda recolección de información personal trae aparejada una obligación de protección de los datos. La responsabilidad por el cumplimiento de las políticas de privacidad, así como por los procedimientos que se realicen al efecto, debe ser documentada y comunicada y debe estar a cargo de personas específicas dentro de la empresa. Cuando transferimos información personal a terceras partes, estas deben disponer de una protección de da-tos equivalente, que puede lograrse ya sea por contratos o por otros medios. Siempre la rendición de cuentas habrá de estar presente.

C. Finalidad. Es necesario especificar el propósito para el cual la información es acopiada, usada, retenida, exhibida, y comunicar esta finalidad al titular del dato en el momento en que esta es recolectada. La finalidad debe ser clara, delimitada y proporcional a las circunstancias.

D. Limitaciones a la recolección. La colecta de información personal debe ser realizada de buena fe, conforme lo indican las normas, y debe estar limitada a los datos necesarios para la finalidad específica.

Los datos personales que se colectan deben ser los estrictamente necesarios. En principio, el diseño de programas, la participación de las tecnologías de la información y la arquitectura de los sistemas deben encauzarse por medio de interacciones y transacciones que no permitan asociar los datos con sus titulares, atendiendo a su anonimización. Deben agotarse los esfuerzos

tendientes a evitar la asociación, identificación y exposición del titular del dato.

E. Limitaciones en el uso, la retención y la divulgación. Es necesario que el uso, la retención y la divulgación de los datos se vean limitados a la finalidad que fuera explicitada al titular del dato, con las únicas excepciones previstas por la ley.

Los datos personales debe ser retenidos sólo durante el lapso necesario para la finalidad y a posteriori esa información debe ser totalmente destruida.

F. Precisión. Los datos personales deben ser conservados en forma completa, precisa y actualizada a efectos de cumplir con la finalidad.

G. Seguridad. Es necesario que el responsable de la base de datos asuma su obligación de brindar seguridad a los datos personales en todo su ciclo de conservación.

Esta seguridad debe ser consistente con los estándares internacionales. Los datos personales deben ser protegidos por medios razonables, que podrán ser físicos, técnicos y administrativos y deberán ser apropiados al grado de sensibilidad del dato.

H. Apertura. La apertura y la transparencia son claves para la rendición de cuentas. De ahí que es preciso proveer a los titulares del dato de información acerca de las políticas de privacidad y de las prácticas que tienen relación con el manejo de sus datos personales.

I. Acceso. Debe suministrarse a todo titular del dato acceso a su información personal e informársele, asimismo, del uso y la exposición que se dará a su dato.

Todo titular del dato debe poder verificar la precisión del mismo y exigir su corrección si fuera necesario.

J. Cumplimiento. Es necesario establecer mecanismos de queja y comunicarlos abiertamente. En la comunicación deben

incluirse todas las instancias y los pasos a los que se pueden recurrir para obtener la corrección o actualización del dato. Es de importancia, asimismo, que se tomen las medidas necesarias para monitorear, evaluar y verificar el cabal cumplimiento de las políticas de privacidad y los procedimientos. **(Brian Nougrères, 2012, págs. 7-8)**

iv. Principios que rigen el uso de los datos personales

Legalidad

El tratamiento de los datos personales se hace conforme a lo establecido en la LPDP. Se prohíbe la recopilación de los datos personales por medios ilícitos.

Consentimiento o Autorización

Para realizar el tratamiento de los datos personales se debe contar con el consentimiento o la autorización de la persona, titular de los datos personales.

Finalidad

Los datos personales no deben ser tratados para una finalidad distinta a la establecida al momento de su recopilación.

Proporcionalidad

Todo tratamiento de datos personales debe ser apropiado a la finalidad para la que éstos hubiesen sido recopilados, usando la información que sea imprescindible y suficiente, sin excesos.

Calidad

Los datos personales que se tratan deben ser veraces, exactos y adecuados.

Seguridad

El titular del banco de datos personales y el encargado del tratamiento deben adoptar las medidas necesarias para garantizar la seguridad y confidencialidad de los datos personales que administran.

v. El principio de Autodeterminación Informativa

Refiere **(Sar Suarez, 2013, pág. 7)** "El derecho a la autodeterminación informativa, incorporado en el inciso 6º del artículo 2 de la Constitución, **consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros *ya sean públicos o privados, físicos o informáticos***, a fin de enfrentar las posibles extralimitaciones de los mismos."

Explicando lo referente al principio de autodeterminación informativa, se puede decir que parte del derecho de protección de datos personales, veamos **(Ministerio de Justicia y Derechos Humanos, 2014, pág. 5)** "**Es el derecho que toda persona tiene a controlar la información personal que comparte con terceros, así como el derecho a que ésta se utilice de forma apropiada, es decir, de forma que no la perjudique**"

El mencionado derecho de autodeterminación informativa o de protección de datos personales, cuenta con una base constitucional, que ha sido interpretada por el tribunal constitucional, como más adelante se verá, sin embargo conviene recordar **(Ministerio de Justicia y Derechos Humanos, 2014, pág. 5)** "La Constitución Política del Perú en su artículo 2, numeral 6, reconoce el derecho que toda persona tiene a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar."

El tratamiento de la protección de datos personales en relación al principio de autodeterminación informativa, surge en defensa del Art 2, inc. 6 de la constitución como ya se vio, sin embargo, el desarrollo normativo del mencionado precepto constitucional, fue abordado legislativamente en la ley 29733, que es la Ley de protección de Datos Personales, a lo cual añade **(Ministerio de Justicia y Derechos Humanos, 2014, pág. 6)** "La LPDP tiene por objeto garantizar una serie de derechos a las personas, titulares de los datos personales, tales como **el derecho a ser informado de cuándo y por qué se tratan sus datos personales, el derecho a acceder a los datos y, en caso necesario, el derecho a la rectificación o cancelación de los datos o el derecho a la oposición al tratamiento de los mismos**. Para ello, la LPDP establece las reglas, requisitos y obligaciones mínimas que deberán cumplir los titulares de los bancos de datos al recopilar, registrar, almacenar, conservar, transferir, difundir y utilizar datos personales."

Sin embargo en relación al marco brasileño aún quedan muchos puntos por definir, ya que en ningún punto de lo observado, se puede establecer que se haga mención directa a la intimidad de la persona como sustento de la norma.

De lo anterior y en refuerzo de la última idea, en nuestro país se reconoce el derecho de acceso a la información pública y/o el derecho de autodeterminación informativa solo respecto la información pública no a la que los usuarios puedan reclamar o no en Internet en una vía razonable, al respecto, el documento 01887-2012-HD Resolución del **(Tribunal Constitucional, 2013)** define **el derecho de autodeterminación informativa como el derecho que tiene toda persona para ejercer control sobre la información personal**, sobre lo que precisa: "*...consiste en la serie de facultades que tiene toda persona, para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles*

extralimitaciones de los mismos…, …Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, ***sino a la persona en la totalidad de ámbitos****…*"

vi. El principio de Neutralidad

(Wikipedia, 2014) La neutralidad de red o neutralidad de la red es un principio propuesto para las redes de banda ancha de uso residencial y móvil (de las que Internet es el paradigma), y potencialmente aplicable a todas las redes de comunicación, que describe cuál debería ser el tratamiento del tráfico que circula a través de ellas.

Una red neutral es aquella que está libre de restricciones en las clases de equipamiento que pueden ser usadas y los modos de comunicación permitidos, que no restringe el contenido, sitios y plataformas, cantidad de datos descargados, y donde la comunicación no está irrazonablemente degradada por otras comunicaciones.

(Wikipedia, 2014) La red neutral es aquella que permite comunicación de punto a punto sin alterar su contenido… (..) …La posibilidad de regulación para obligar la neutralidad de la red ha sido objeto de debate en numerosos foros. Desde el año 2000 diversos grupos que defienden ciertas normas y la neutralidad de la red han lanzado numerosas campañas con el fin de que los proveedores de servicio no bloqueen aplicaciones y proveedores (por ejemplo, páginas web), particularmente las usadas por la competencia de dichos proveedores.

> Los que proponen la neutralidad aseguran asimismo que las compañías de telecomunicaciones intentan imponer su modelo de servicio para conseguir beneficios aprovechándose del control del servicio, más que por demanda de sus servicios. Otros aseguran que creen que la neutralidad de la red es fundamental para

preservar nuestras libertades. Vint Cerf, co-inventor del Protocolo de Internet, ha asegurado que "***Internet se diseñó sin ningún guardián sobre nuevos contenidos o servicios. Se necesita una regla de neutralidad de red suave pero aplicable para que Internet continúe creciendo***."

Los que se oponen a la neutralidad y a esas normas, por el contrario, llaman a las reglas de Neutralidad de la Red "una solución en busca de un problema" y consideran que las reglas de neutralidad de la red reducirían los incentivos para actualizar las redes y lanzar nuevos servicios de nueva generación. Otros consideran que cierta discriminación de alguna clase —especialmente para garantizar la "calidad del servicio"— no sólo no es negativa, sino deseable. Bob Kahn, coinventor del Protocolo de Internet, ha calificado de eslogan el término "neutralidad de la red", y ha asegurado que se opone a establecerla, avisando que "nada interesante puede pasar dentro de la red" en el caso de que se apruebe tal neutralidad. "Si el objetivo es animar a la gente a construir nuevas capacidades, entonces alguien tiene que dirigir el camino para construir esa nueva capacidad, y probablemente sólo lo va a hacer en su red, no en la red de otros". **(Wikipedia, 2014)**

Clases de transmisores de Internet

En los Estados Unidos se les conoce como "carriers" o "empresas transmisoras" las mismas que se dividen en:

"Transmisores comunes": son de por sí neutros (de ahí el término "neutralidad") puesto que ***brindan un servicio esencial***. Estas entidades tienen permitido cobrar al usuario residencial para mantener su economía, pero, hipotéticamente, ***se les prohíbe modificar la neutralidad según conveniencias privadas***. Es decir, no pueden decidir qué tipo de

contenido circula, salvo que este atente contra el bien común. Por ejemplo los ISP[11] o las compañías de electricidad. **(Wikipedia, 2014)**

"Transmisores privados": prestan servicios no esenciales entre privados, el estado no los regula. Estas empresas deciden su contenido, sin rendirle cuenta a nadie más las fluctuaciones de su propia economía. Ej. TV por Cable y las compañías de telefonía móvil. **(Wikipedia, 2014)**

Los ISP quieren pasar de ser "Transmisores comunes" como han sido considerados históricamente a ser "Transmisores Privados", de ese modo lograr mayor injerencia sobre qué circula en sus redes. Este concepto está causando una considerable controversia en los Estados Unidos, con diferentes iniciativas legislativas destinadas a regular y aplicar, en su caso, dicho principio. **(Wikipedia, 2014)**

Iniciativas legales clasificadas por países

Chile: en julio de 2010, se convierte en el primer país del mundo en aprobar una ley (ley N° 20.4532) a favor de la neutralidad en la red.

Países Bajos: primer país europeo en aprobar una norma de neutralidad, prohibiendo a los operadores de telefonía móvil bloquear o cobrar a los consumidores una tarifa extra por el uso de servicios determinados. En este sentido,...***no podrán ni restringir ni cobrar adicionales por el uso que los consumidores hagan de aplicaciones como skype o WhatsApp***. **(Wikipedia, 2014)**

Ecuador: en el 2012, expidió un Reglamento que en su Art. 15 numeral 6 dice: "Hacer uso de cualquier aplicación o servicio legal disponible en la red de Internet, con lo cual el servicio que ofrezcan los prestadores de los servicios no deberán distinguir ni priorizar de modo arbitrario contenido, servicios, aplicaciones u otros basándose en criterios de propiedad, marca, fuente de origen o preferencia".

---

[11] *Internet Service Provider (ISP) o Proveedor de Servicios de Internet.*

Europa: En 2014 el Parlamento Europeo votó a favor de la neutralidad en la red.

Brasil: En 2014 Brasil aprobó el Marco Civil de Internet, que recoge como principio la neutralidad de la red.

El presidente de Norteamérica señaló respecto a la neutralidad:

"***Obama ha recordado que los principios de libertad y neutralidad rigen Internet desde su creación, pero que no pueden darse por sentados.*** Por eso, asegura que el deber de la FCC, como agencia independiente que es, es crear un nuevo conjunto de normas que protejan esa neutralidad, la amplíen a las conexiones a través de teléfonos móviles, y garanticen que ni las compañías telefónicas ni las operadoras de cable puedan acabar con ella. En su comunicado, Obama también ha presentado un plan de acción en el que propone una serie de normas básicas que ha calificado de sentido común, como por ejemplo la de impedir que las operadoras puedan bloquear al acceso a cualquier web o servicio de contenido legal. Después de todo, la decisión de en qué webs informarse, disfrutar de contenido en streaming, o hacer sus compras online debería recaer siempre en el usuario." **(Genbeta, 2014)**

vii. El principio de Neutralidad Tecnológica

El concepto de neutralidad tecnológica surge de la relación estado – proveedor de Internet, veamos:

"se usa preferentemente a la hora de **describir la actitud que se espera por parte de la Administración Pública en relación con sus proveedores, sobre todo tratándose de proveedores de bienes y servicios informáticos**. Hay quien entiende la neutralidad tecnológica como la igualdad de concurrencia de los proveedores ante el mercado de la Administración Pública. Otra acepción se refiere a la actitud que

debe tomar la Administración Pública respecto de un proveedor que en el transcurso del tiempo ha adquirido respecto de la Administración Pública una situación privilegiada, y de cuyos productos no podría prescindir sin arrastrar grandes costes. Desde el punto de vista del usuario, o del administrado, y especialmente en el ámbito de la Administración electrónica, la neutralidad tecnológica implica que dicho administrado debe poder dirigirse a la Administración Pública por vías telemáticas sin que le sea impuesta, de facto o explícitamente, ningún tipo de tecnología específica". **(Puyol, 2015)**

De otro lado, se puede señalar que: "*la* ***neutralidad tecnológica también se usa como la característica de una ley que enuncia derechos y obligaciones de las personas sin disponer nada acerca de los medios tecnológicos necesarios para que se cumplan. Se trata de leyes que se desinteresan del marco tecnológico. La segunda acepción es la que está ganando más terreno en el idioma, y está íntimamente ligada a la política respecto de los monopolios*****". (Puyol, 2015)**

El término "neutralidad tecnológica", al parecer ***proviene de la Ley Modelo de la CNUDMI (UNCITRAL)***[12] sobre Comercio Electrónico de 1996, la cual establece: "***Al incorporar a su derecho interno los procedimientos prescritos por la Ley Modelo para todo supuesto en el que las partes opten por emplear medios electrónicos de comunicación, un Estado estará creando un entorno legal neutro para todo medio técnicamente viable de comunicación comercial***". Este principio ha sido reiterado en otros cuerpos legales, como la Ley de Chile número 19.799 sobre sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, donde se hace referencia a la neutralidad tecnológica en el mismo contexto.

[12] *Significa: Comisión de las Naciones Unidas para el derecho mercantil internacional (CNUDMI) o UNCITRAL por su siglas en inglés "United Nations Commission for the Unification of International Trade Law"*

En este sentido, debe indicarse que ***la ley no se restringe a una tecnología particular, sino que se formula de tal manera que se aplica a cualquier tecnología que corresponda, ahora o a futuro***, al problema que se está legislando. **(Puyol, 2015)**

Señalado lo anterior tenemos:

"En este caso, la firma, que puede ser digital o en papel, entre otros medios, y es el reglamento el que va estableciendo los aspectos específicos a la tecnología. Consecuentemente con ello, para habilitar una tecnología nueva no es necesario modificar la ley. Posteriormente, en la Cumbre Mundial sobre la Sociedad de la Información, organizada por la Unión Internacional de Telecomunicaciones (ITU), que constituye una organización internacional integrante de Naciones Unidas, se señala que dentro de sus principios fundamentales la necesidad de un "entorno propicio", y al amparo de este concepto, en su Artículo 39 ***se indica la necesidad de la existencia de un estado de derecho, acompañado por un marco de política y reglamentación propicio, transparente, favorable a la competencia, tecnológicamente neutro, predecible y que refleje las realidades nacionales***, es insoslayable para construir una Sociedad de la Información centrada en la persona. ***Los gobiernos deben intervenir, según proceda***, para corregir los fallos del mercado, mantener una competencia leal, atraer inversiones, intensificar el desarrollo de infraestructura y aplicaciones de las TIC, aumentar al máximo los beneficios económicos y sociales y atender a las prioridades nacionales" **(Puyol, 2015)**.

En sintonía con lo ya referido, tenemos:

"Cullel señala que una de las primeras referencias al principio de neutralidad tecnológica se encuentra como principio de regulación en el año 1999 en un documento oficial de la Comisión Europea sobre la revisión del marco normativo de las comunicaciones electrónicas. Este principio se adoptó como uno de los cinco principales que regían el marco regulador de las comunicaciones electrónicas en la UE. Según este documento, ***la neutralidad tecnológica supone que la legislación debe definir los objetivos a conseguir sin imponer ni discriminar el uso de cualquier otro tipo de tecnología para conseguir los objetivos fijados***. El concepto de neutralidad tecnológica, según Koops se debe diferenciar del de independencia tecnológica, que como su

nombre indica es totalmente independiente de una determinada tecnología y no establece ningún tipo de enlace con los aspectos tecnológicos **(Puyol, 2015)**.

Extendiendo lo expuesto, tenemos:

"El principio de neutralidad tecnológica como principio de regulación ***debe inspirar la actividad reguladora de las autoridades nacionales, que pretende conseguir unos determinados efectos, es decir, la regulación tecnológica debe prestar atención a los efectos de las acciones y no a las acciones y a los medios por ellos mismos***. Esta premisa aplicada al ámbito tecnológico supone que la actividad reguladora, lejos de centrarse en la tecnología, presta atención a los efectos que emanan de su uso, por ello, la técnica legislativa debe basarse en una regulación sostenible, subsidiaria y proporcionada a la vez que transparente. A su vez, ***la regulación inspirada en el principio de neutralidad debe evitar efectos de discriminación entre otras tecnologías al mismo tiempo que favorecer el desarrollo de las TIC***" **(Puyol, 2015)**.

Un aspecto importante a destacar es el que supone la neutralidad en el acceso y la libertad de elección, como se verá a continuación:

"Boix apunta que la idea de neutralidad tecnológica es, en el fondo, algo más sencillo, aparentemente menos ambicioso que la aspiración de generalizar el derecho a poder acceder a cualquier procedimiento por vía electrónica, pero igualmente importante: se trata, en sentido estricto, de garantizar que los medios tecnológicos empleados por el ciudadano, o que éste tenga a su disposición, tengan un efecto neutro en la tramitación del procedimiento. Es decir, que el decantarse por uno u otro no conlleve efectos en positivo o en negativo de ningún tipo, ni, por supuesto, merma de garantías. De tal manera que la elección por de unos u otros no esté condicionada por beneficios regulatorios en favor de algunos y detrimento de otros, sino por meras consideraciones de comodidad o preferencia personal. La ley, en este sentido, consagra esta idea como uno de sus criterios angulares, al señalarla como uno de los principios rectores que han de inspirar la práctica administrativa en la materia en su artículo 4. i): Art. 4. i) Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas garantizando la independencia en la elección de las alternativas tecnológicas por

los ciudadanos y por las Administraciones Públicas, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las Administraciones Públicas utilizarán estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos" **(Puyol, 2015)**.

Es necesario señalar la neutralidad a la hora de comunicarse con un organismo de la administración pública, como se verá:

> "La previsión es importantísima, en los términos en que la Ley se expresa, pues establece como principio rector la idea de que cualquier ciudadano ha de poder comunicarse con la Administración en igualdad de condiciones con independencia del sistema o medios técnicos que utilice, en lo que abundan derechos como el del artículo 6.2 k) de la ley, que garantiza a los administrados la posibilidad de "elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos" **(Puyol, 2015)**.

Sin embargo, ***la referencia a la neutralidad tecnológica como criterio rector de la ley va más allá, aunque no esté explícitamente reflejado de esta manera. Cuando la ley garantiza también la igualdad entre el procedimiento electrónico o cualquier otro, toda la regulación destinada a lograr este objetivo es también reflejo de esta misma idea*** **(Puyol, 2015)**.

Como detalle conclusivo, se llega al fondo del asunto al señalar que la neutralidad tiene como propósito el indiferenciar la preferencia del usuario en usar la tecnología virtual y sus ya acostumbrados trámites presenciales o físicos, atendamos la siguiente explicación:

> "Simplemente, se trata de una situación en la que ***la neutralidad ha de lograrse no entre diversas variantes de una misma tecnología (Windows, Linux o Mac, por ejemplo; tal o cual programa para acceder a Internet o para procesar texto, etc.) sino entre dos opciones de "tecnología de comunicación" radicalmente diferentes: la presencial o la electrónica***. La ley no

se refiere cuando habla de neutralidad tecnológica a esta cuestión, ya que ciñe expresamente el concepto a una definición estricta, por mucho que a lo largo de su articulado hay una evidente preocupación por la misma que es perfectamente homologable. En el fondo, el gran objetivo de la norma es consagrar y garantizar también este tipo de neutralidad tecnológica entendido en sentido amplio, por mucho que no le denomine de esta forma **(Puyol, 2015)**.

Complementando lo ya explicado, **(Stallman, 2014)** refiere: "***Los desarrolladores de software privativo que se oponen a las leyes que promueven la migración al software libre a menudo sostienen que tal medida es contraria al principio de «neutralidad tecnológica»***. Esta conclusión es errónea, ¿pero dónde está el error?"

Al respecto de lo señalado, se explica el porqué del error antes observado, veamos:

> "El principio de la neutralidad tecnológica consiste en que el Estado no ha de imponer preferencias a favor o en contra de una determinada tecnología. Por ejemplo, no debe existir ninguna regla que especifique si los organismos estatales deberían utilizar memorias de estado sólido o discos magnéticos, o si tienen que usar GNU/Linux o BSD. Más bien, el Gobierno debe permitir que los licitadores propongan cualquier tipo de tecnología aceptable como parte de las soluciones que ofrecen, y optar por la oferta mejor o menos costosa según los procedimientos habituales" **(Stallman, 2014)**.

En relación al entorno, como bien es sabido toda actividad humana causa un cambio en la naturaleza, es así que podemos señalar lo siguiente: "El principio de la neutralidad tecnológica es válido, *pero tiene sus límites. Algunas tecnologías son perjudiciales: pueden contaminar el aire o el agua, favorecer la resistencia a los antibióticos, causar daños a los usuarios o a los trabajadores que las fabrican, o provocar una situación de desempleo masivo.* ***Tales tecnologías deberían estar***

***sujetas a gravamen y regulación, y deberían ser desalentadas o incluso prohibidas*" (Stallman, 2014).**

***El principio de la neutralidad tecnológica se aplica únicamente a las decisiones de orden técnico. No se trata de «neutralidad ética» o «neutralidad social». No se aplica a las decisiones sobre cuestiones éticas o sociales, como la opción entre software libre y software privativo* (Stallman, 2014).**

Un ejemplo de lo ya descrito supone una decisión gubernamental como se explicará más adelante:

"Por ejemplo, cuando el Estado adopta una política de migración al software libre para restaurar la soberanía informática del país y promover la libertad y la cooperación entre los ciudadanos, no es una preferencia técnica. Se trata de una decisión de orden ético, social y político, no tecnológico. ***Se supone que el Estado no debe ser neutral a la hora de preservar las libertades individuales y promover la cooperación. Se supone que no ha de ser neutral con respecto a la preservación o restauración de su soberanía*" (Stallman, 2014).**

Ampliando lo ya observado tenemos que:

> "Es deber del Estado insistir en que el software utilizado por los organismos estatales respete la soberanía informática del país, y que el software que se enseña en las escuelas eduque a los alumnos para la libertad y la cooperación. El Estado debe insistir en el uso exclusivo de software libre en los organismos públicos y en la educación. Es responsabilidad del Estado mantener el control de sus actividades informáticas, por lo que no debe renunciar a este control delegándolo en el servicio sustitutivo del software (SaaSS)[13]. Además, el Estado no debe revelar a las empresas los datos personales de los ciudadanos" **(Stallman, 2014)**.

[13] *Saas es aquella aplicación ofrecida por su creador (ISV) a través de internet para su uso o utilización por varios clientes manteniendo la privacidad de sus datos y la personalización de la aplicación.*

Ultimando la secuencia de ideas se puede decir que: "Una decisión técnica compete al ámbito de la neutralidad tecnológica cuando no involucra aspectos éticos" **(Stallman, 2014)**.

B. Derecho a la intimidad y el derecho a la autodeterminación informativa

Un hecho ya explicado es el concerniente a la dignidad de la persona como fundamento de su desarrollo, de cual parte o surge la intimidad como derecho, esta a su vez vela o tiene su razón de ser en el pleno desarrollo que la persona necesita para ser completa, esto naturalmente está garantizado por derechos que permiten a la persona la capacidad de actuación plena sin intromisiones ajenas, para ello señala **(Herrán Ortiz, 2003, pág. 9)** "**la autodeterminación que nace de la libre proyección humana, y que se encuentra vinculada a la idea de intimidad personal y familiar**"

> Los derechos humanos se clasifican en generaciones, Pérez-Luño considera que el cambio generacional de los derechos humanos atiende al contexto histórico y situación humana que así lo reclamó y que los derechos humanos se encuentran en constante evolución; en este sentido cada generación no termina cuando inicia la siguiente sino cada nueva generación refuerza a la anterior y así sucesivamente; un ejemplo de ello es el derecho a la intimidad y su evolución, ya que forma parte de los derechos de la primera generación en donde se reconocieron las libertades individuales, la segunda generación surge a consecuencia de las luchas sociales, por lo que se tuvo la necesidad de reconocer no solo los derechos individuales sino los económicos, los sociales y los culturales, en este sentido el derecho a la intimidad no sufrió ningún cambio; sin embargo el reconocimiento de la tercera generación de derechos, reivindicó el derecho a la intimidad, ya que surgen como una respuesta a la denominada "liberties´ pollution o contaminación de libertades" es así como surgen, el derecho a la paz, el derecho a la calidad de vida, el derecho a la libertad informática el cual se encuentra íntimamente ligado con el

derecho a la intimidad entre otros **(Álvarez Rodríguez, 2012, págs. 106-107)**.

En este orden de ideas la preocupación por los datos personales se da a partir de la Declaración de Teherán de 1968 al establecer en una de sus cláusulas que los avances científicos y tecnológicos son importantes para el desarrollo económico, social y cultural de los países, sin embargo estos avances pueden atentar contra derechos fundamentales; es decir la autodeterminación informativa surge cuando se fue consciente de que utilizando las nuevas tecnologías era posible almacenar una gran cantidad de información y además de ello se sometía a tratamiento informatizado, dicho tratamiento suponía un riesgo a la intimidad es por eso que se configura como garantía y medio de defensa para tener control de la información personal que se encuentra en registros públicos y privados almacenados en medios informáticos **(Álvarez Rodríguez, 2012, pág. 107)**.

C. Intimidad, seguridad jurídica y el derecho Informático

Como se ha venido diciendo de un modo redundante, hoy el avance tecnológico y el desarrollo comunicativo son las características que definen a nuestra sociedad actual, ante el escenario descrito, resulta evidente que uno de los campos que más ha contribuido al desarrollo es la Informática y "en general todos los aspectos que pueden englobarse bajo el término "Sociedad de la Información" presentan una serie de características especiales y poseen la entidad suficiente como para justificar un desarrollo normativo específico" **(Zaballos Pulido, 2013, pág. 41)**.

Siguiendo el orden de ideas, la relación entre Informática como productor del cambio y el Derecho como garante de las reglas de la sociedad se manifiesta en múltiples aspectos veamos:

- Uso de nuevas vías para la celebración de contratos.
- Empleo de medios probatorios más seguros y adecuados a las necesidades demandadas por la sociedad.
- La generación (y a su vez, necesidad de protección adecuada) de una nueva modalidad de bienes que ha derivado en la aparición de un nuevo tipo de propiedad industrial sobre los programas de ordenador.

(Zaballos Pulido, 2013, pág. 41)

i. El Derecho Informático

Para Julio Téllez Valdés, el Derecho Informático es... "Una rama de las ciencias jurídicas que considera a la Informática como instrumento (Informática Jurídica) y objeto de estudio (Derecho de la Informática)."

Puede definirse como la aplicación del conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y las comunicaciones y que tiene por objeto la aplicación de las Tecnologías de la Información al Derecho.

Se trata de un ámbito que, debido sus aspectos regulatorios, debe ser dinámico en cuanto a la evolución de la tecnología y en segundo lugar pone de manifiesto la ruptura de fronteras su carácter internacional "se encuentra por un lado, en permanente evolución exigiendo un esfuerzo constante de adecuación a los nuevos riesgos y necesidades y por otro lado es una materia en la que hay que tener siempre muy presente la regulación a nivel internacional y europeo, ya que su objeto es la regulación de actividades que tienen como una de sus principales características, su capacidad para rebasar fronteras". **(Zaballos Pulido, 2013, pág. 41)**

En el contexto español, las bases de este novedoso derecho se hallan en su texto constitucional, **(Zaballos Pulido, 2013, pág. 41)** expresa: "En España, la base del Derecho Informático es el

reconocimiento constitucional del uso de la informática, con las limitaciones que se establezcan legalmente (artículo 18.4 de la Constitución Europea)".

Dichas normas, han propiciado "que algunos autores comiencen a hablar del Derecho informático, como una rama autónoma e independiente del ordenamiento. De acuerdo con este planteamiento, quedarían comprendidos dentro del derecho informático, entre otros, los siguientes aspectos":

- Telecomunicaciones
- Protección de Datos.
- Delitos informáticos.
- Responsabilidad civil en materia informática.
- Firma Electrónica.
- Contratación informática y electrónica
- Creación, distribución, explotación y utilización de hardware y software.
- Protección del honor, la intimidad personal y familiar y la propia imagen.
- Servicios y entorno de la Sociedad de la información.

(Zaballos Pulido, 2013, pág. 42)

ii. Indefensión jurídica

Definiendo lo que significa indefensión jurídica tenemos **(Wikipedia, 2013)**, "La indefensión es un concepto jurídico indeterminado **referido a aquella situación procesal en la que la parte se ve limitada o despojada por el órgano jurisdiccional de los medios de defensa que le corresponden en el desarrollo del proceso**. Las consecuencias de la indefensión pueden suponer la imposibilidad de hacer valer un derecho o la alteración injustificada de la igualdad de medios entre las partes, otorgando a una de ellas ventajas procesales arbitrarias.

La **(Enciclopedia Jurídica, 2014)** define: "**Situación en la que queda una parte del proceso cuando se le impide el ejercicio de un derecho de naturaleza procesal, anulando o restringiendo, total o parcialmente, sus oportunidades de defensa**. La indefensión **puede dar lugar a la nulidad** de lo actuado y es motivo para recurrir las resoluciones judiciales. **Es la situación en que se encuentra quien no ha sido defendido o no se ha defendido, sin culpa por su parte, en un juicio que lo afecta**. Esa indefensión **vulnera el principio de la inviolabilidad de la defensa, que suele presentar una garantía constitucional**. Esta norma resulta particularmente importante en materia penal, ya que ni siquiera queda librado a la voluntad del imputado el derecho de no defenderse. Si él no designa defensor, el tribunal está obligado a nombrarle uno de oficio."

Ante el derecho comparado, específicamente en España, **(Wikipedia, 2013)** la indefensión: "**supone la vulneración de los derechos fundamentales procesales** recogidos en la Constitución del 78, concretamente en su artículo 24.1. No obstante, es jurisprudencia reiterada del Tribunal Constitucional que **no se puede aceptar el amparo por indefensión cuando quien la sufre se haya colocado con su actuación voluntaria o negligente en tal situación.**"

D. La intimidad en la red

Un pequeño resumen de los que supone la intimidad y su evolución en el tiempo, los detalla **(Emparan Legaspi, 2012, págs. 4-5)**, "Privacidad, de acuerdo con el Diccionario de la Lengua Española de la Real Academia, es el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión", es decir, lo íntimo. De acuerdo con Aristeo García (2007, p. 748), en el siglo XVIII, autores como John Stuart Mill, Samuel Warren y Luis Brandeis configuraron el llamado "derecho a la intimidad", que es, precisamente, el derecho de mantener para uno mismo ese "ámbito de la vida privada", el cual pertenece únicamente a nosotros

y, si acaso, a nuestra familia. Para Stuart Mill, dice García González (2007, p. 749), la intimidad era el derecho a buscar la felicidad a nuestra propia manera, mientras que para Warren y Brandeis, en su obra The Right of privacy, era el derecho a la soledad y a la protección de la persona frente a cualquier intromisión en su vida privada y doméstica. Brandeis, como juez de la Suprema Corte de los Estados Unidos, promulgó en 1890 una ley que buscaba proteger a los ciudadanos de cualquier intromisión por parte del gobierno o de otro miembro de la sociedad (García, 2007, p. 750). Después de la promulgación de la Ley en Estados Unidos, el derecho a la intimidad se estableció como un derecho fundamental de todo ser humano".

E. Límites de la protección de la intimidad

i. El secreto de las comunicaciones

Una de las formas de comunicación moderna es a través de la línea telefónica, con mayor razón, en la última década, con la amplia difusión de la telefonía celular.

> Este es uno de los medios más usados para conocer de hechos concernientes a la esfera de la intimidad de las personas. Los secretos mejor guardados se revelan en una comunicación telefónica, por lo tanto, constituye una proyección del derecho a la intimidad este tipo de comunicaciones175. La violación de la comunicación telefónica puede tener diversas motivaciones, de orden político, económico, financiero, investigaciones privadas, etc., pero ninguna de ellas estará justificada si es que no existe un interés superior que esté en juego y que constituye un limitante a la intimidad de la persona. Por todos es conocido que en la última década, una de las formas de controlar y ejercer presión sobre determinados personajes de la política nacional o del ambiente artístico no solo han sido los videos que se grabaron, sino las interceptaciones telefónicas. Nuestro sistema jurídico protege la comunicación telefónica y lo hace a través de la Constitución Política del Estado. Sin embargo, conviene recalcar que la Constitución de 1993 no hace distingo entre la comunicación telefónica de las demás formas de comunicación, protegiéndolas

> igualmente a todas, pero relativizándolas, esto es, permitiendo la interceptación por mandamiento motivado de juez, con las garantías previstas en la ley. Añade luego que los documentos privados obtenidos con violación del precepto anteriormente mencionado, no tienen efecto legal. Debe entenderse que también comprende la comunicación telefónica interceptada sin mandato judicial. **(La Constitución Comentada, 2005, pág. 171)**

Similar situación se desarrolla en España pues la tratativa de la intimidad en relación al secreto de las comunicaciones se desenvuelve de manera análoga, veamos:

Otro ámbito típico del derecho a la intimidad ***es el secreto de las comunicaciones en la medida en que es –o puede ser- medio de conocimiento de aspectos de la vida privada.*** El artículo 18 de la Constitución Española garantiza también el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas salvo resolución judicial. **(Herrera de Egaña, 2007, pág. 11)**.

ii. Los datos sensibles

Nuestra legislación precisa **(Ministerio de Justicia y Derechos Humanos, 2014)** "Dentro de los datos personales hay una categoría denominada "datos sensibles" que están constituidos por:

- Los datos biométricos que por sí mismos pueden identificar a la persona, como la huella digital, la retina, el iris;
- Datos referidos al origen racial y étnico;
- Ingresos económicos;
- Opiniones o convicciones políticas, religiosas filosóficas o morales; la afiliación sindical;

Información relacionada a la salud o a la vida sexual. Estos datos requieren de especial protección y solamente pueden ser objeto de tratamiento con el consentimiento expreso y por escrito del titular de los datos".

(Miranda P., 2014) Señala refiriéndose a los datos sensibles en la realidad costarricense: La Corte Suprema de Justicia dictó las reglas con las que protegerá los "datos sensibles" en todas las sentencias judiciales. ***La entidad evitará que terceras personas tengan acceso (por Internet u otro medio) a información como las creencias religiosas, orientación sexual o filiación política de los involucrados en procesos judiciales***.

Lo señalado obedece al cuerpo legal en defensa de los datos personales o específicamente los datos sensibles de las personas, denominado Ley de Protección de la Persona frente al Tratamiento de sus Datos, cuyo reglamento se emitió el 11 de agosto del 2014.

En cumplimiento con lo señalado, el juez costarricense Carlos Chinchilla, señala que cada sentencia experimenta un proceso de despersonalización, en atención al equilibrio que debe existir entre la protección de datos personales (datos sensibles) y el derecho de acceso a la información, por ello explicando y extendiendo el tema:

> "El funcionario enfatizó que no se trata de "ocultar todo" y admitió que en algunas áreas de la institución todavía hay desconocimiento sobre el tema. Según criterio de Chinchilla, esa ***despersonalización (eliminar los datos que identifican a la persona) solo debe hacerse cuando el fallo contenga otras informaciones consideradas sensibles o personales de carácter privado***. "Según fallos de la Sala Constitucional, hay datos personales que no se pueden divulgar, como teléfonos privados o la dirección." Pero también existen los datos sensibles, que son el punto medular de la ley. ¿Cómo se identifica un dato sensible? Es aquel que puede discriminar o excluir de la sociedad o de un grupo social", explicó Chinchilla". **(Miranda P., 2014)**

En añadidura a lo visto en el párrafo antepuesto y explicando el mecanismo de despersonalización de la información íntima, contenida en una sentencia, de ello el juez Carlos Chinchilla refiere estableciendo los parámetros referidos a cada actor que ocupa la sentencia:

"...para que se realice la despersonalización primero el juez o tribunal que dicta la sentencia, debe enviarla a un repositorio digital, con la alerta de que podría contener datos sensibles. "Eso manda la resolución a un recipiente que lo centraliza en el Digesto de Jurisprudencia (oficina que respalda los fallos)", detalló. ***Los funcionarios de dicho departamento revisarán cada texto para determinar si, efectivamente, corresponde suprimir datos. "La información sensible va a permanecer, porque es una guía jurisprudencial importante, pero se despersonaliza la identificación. Casi siempre se trata de víctimas, de agresiones sexuales, delitos contra menores***, dijo Chinchilla. "Por ejemplo, una persona acusada de agresión sexual contra persona menor es condenada a 20 años de prisión. Entonces la gente dice: ¡Qué terrible!, si se publica no le van a dar trabajo en ningún sitio; entonces, ¿hay que despersonalizarle la sentencia? No. ***De esa sentencia despersonalizo a las víctimas, no al imputado*** ni lo que hizo", agregó". **(Miranda P., 2014)**

En concordancia a lo que establece la norma de protección de datos personales, el juez Carlos Chinchilla señaló que existen algunos inconvenientes a la hora de aplicar la norma, pues las sentencias judiciales tienen un carácter dinámico en relación a lo que dictamina la norma, veamos:

El magistrado dijo que se mantendrá una base interna con la información completa. Reconoció que, por el momento, el Poder Judicial no cuenta con la tecnología para modificar las sentencias orales, pero argumentó que son pocas las que no tienen respaldo escrito y se va a buscar la forma de hacerlo. Chinchilla informó, además, de que se contrató a una firma extranjera para despersonalizar 40.000 fallos que se dictaron en un plazo que dio la ley cuando entró en vigencia y que vencía en marzo del año pasado. Sin embargo, indicó que el resultado no fue el esperado porque se tendió a ocultar "todo" y no se ha dado por recibido el producto. **(Miranda P., 2014)**

iii. Los datos íntimos no patrimoniales

El tratadista Manuel Egaña se refiere a los denominados datos íntimos no patrimoniales, como aquellos que maneja la administración

tributaria, en relación al cumplimiento de las obligaciones, al respecto amplía: "Como antes se ha visto, la Administración tributaria está habilitada legalmente para solicitar de cualquier persona ***datos relacionados con el cumplimiento de sus propias obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras con otras personas que tengan trascendencia tributaria*** que, según se ha visto, puede ser indirecta, potencial o hipotética **(Herrera de Egaña, 2007, pág. 10)**.

Así mismo lo dicho anteriormente se refuerza: "***los datos referidos a la actividad económica de una persona no tienen en sí relevancia para la intimidad personal y familiar del contribuyente*** aunque, si llegaran a tenerla, primaría el deber de contribuir frente al derecho a la intimidad". **(Herrera de Egaña, 2007, pág. 10)**

Por ello en el contexto español, la norma excluye de la obligación de suministro a "***la información referida a "los datos privados no patrimoniales que conozcan por razón del ejercicio de su actividad cuya revelación atente contra el honor o la intimidad personal y familiar***"." **(Herrera de Egaña, 2007, pág. 10)**

iv. El derecho al olvido y la autodeterminación informativa en las redes sociales

El derecho a la protección de datos personales, libertad informática o derecho a la autodeterminación informativa, en el contexto de la sociedad de la información, supone la aplicación de las nuevas tecnologías en los más variados ámbitos de las actividades humanas; prueba de ello es el impacto global de las redes sociales en internet, que son plataformas que permiten interactuar a los usuarios mediante el intercambio de diversos contenidos (mensajes, archivos, imágenes, música, videos, entre otros). Las redes sociales en internet, constituyen un medio de comunicación primordial para establecer relaciones

personales, como es el caso de facebook (red global con mayor número de usuarios, cerca de 450 millones); el indicador de la sociedad de la información (ISI). En este sentido nos permite vincularnos con amigos del mismo contexto social o reencontrarnos con amigos del pasado e inclusive es un medio para encontrar pareja o twitter que permite a los usuarios allegarse de información que sea de su interés en cuestión de segundos; es decir, la red es ajena a fronteras territoriales, cualquier tipo de información, dada la rapidez de internet circulan de manera masiva sin que podamos tener control sobre ella una vez que se encuentre en el ciberespacio. **(Álvarez Rodríguez, 2012, pág. 4)**

Como usuarios de las redes sociales nuestros datos personales quedan expuestos al conocimiento público lo que trae como consecuencia una invasión a la intimidad que es donde se configura la esencia de la persona, lo que lo hace único ya que sus actuaciones, sentimientos o pensamientos solo se pueden percibir si el sujeto los exterioriza mediante sus actuaciones o sus palabras, es decir con la publicación de creencias religiosas, filosóficas y morales, opiniones políticas dejamos al descubierto aspectos que son considerados datos sensibles.

Sin embargo tenemos la libertad de decidir qué información compartimos con las demás personas y cual no, en este sentido, surge la preocupación por tener mayor control de la información que publicamos, de ahí que deriven cuestionamientos relacionados con el tratamiento que se les da a nuestros datos personales; es decir, preguntas como:

¿Cuánto tiempo permanecen mis datos en la red una vez que haya desactivado mi cuenta?

¿Qué sucede con mis datos cuando dejo de ser usuario de una red social?

¿Puedo disponer del contenido que se sube a la web y que atente contra mi honra, imagen o causen un deterioro a mis relaciones personales, sociales y labores?

La realidad tecnológica continúa rebasando el mundo jurídico, por lo que se debe captar esa realidad en pos de tutelar por sobre todas las cosas la dignidad humana; en este sentido la Unión Europea (UE) tomando en consideración la carta de los derechos fundamentales a través de la comisión de justicia, derechos fundamentales y ciudadanía presentará en este año: [...] propuestas legislativas destinadas a revisar el marco jurídico de la protección de datos, con el objetivo de reforzar la situación de la Unión Europea (UE) en materia de protección de los datos personales (Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones), así mismo se adoptarán otros instrumentos jurídicos. **(Álvarez Rodríguez, 2012, pág. 5)**

En este orden de ideas se pretende regular el derecho al olvido en internet, que consiste en borrar el pasado de una persona que pudiere resultar vergonzoso o afectarlo de alguna manera, así como su indexación en los principales buscadores como Google para recuperar y controlar nuestra información se tendrá el derecho de retirar su consentimiento al procesamiento de datos y exigir que sean borrados completamente cuando dejen de ser necesarios para los fines que se recabaron o cuando los usuarios se den de baja del servicio, esta reforma tendrá como pilares fundamentales la transparencia, la privacidad por defecto y el derecho a ser olvidado. Los avances tecnológicos y la globalización han transformado la sociedad, internet es una herramienta indispensable para las actividades que realizan los Estados y las personas, las redes sociales forman parte importante de este cambio, por lo que debe existir regulación jurídica que atienda a estas nuevas necesidades sociales, incluso, cuando no se ha materializado la incorporación del derecho al olvido en la

legislación Europea, pretende ser un mecanismo jurídico que garantizará la autodeterminación informativa de las personas, lo que permitirá tener mayor seguridad jurídica y confianza al ser usuario de una red social. **(Álvarez Rodríguez, 2012, págs. 6-7)**

F. El derecho a la privacidad

Con el devenir de los tiempos el uso cada vez más intensivo de Internet, ha incrementado la presencia del usuario en la red o nube, una pequeña proyección de ello, la señala **(ESET-Latinoamérica, 2014, pág. 5)**, "la tendencia indica un crecimiento en al almacenamiento de información en la nube, es decir, el uso de esta tecnología por parte de los usuarios va aumentando conforme pasa el tiempo. En el caso de América Latina, el crecimiento porcentual que se proyecta para 2017, en comparación a los años anteriores, es de un 31%. Esta tendencia de "ir hacia la nube" por supuesto que tiene implica a la seguridad de la información, pero además existe una cuestión que en los últimos años ha sufrido algunas modificaciones dado el uso que las personas le han dado a la tecnología, y es el tema de la privacidad."

La privacidad **es el interés que los individuos tienen en sostener un espacio personal, libre de interferencias con otras personas y organizaciones (El rincon del vago, 2004)**.

Privacidad de Personas

La privacidad de la persona, designada a veces como "aislamiento corporal" se refiere a la integridad del cuerpo del individuo. **(El rincon del vago, 2004)**

Privacidad del Comportamiento Personal

Esto se relaciona con todos los aspectos del comportamiento, pero especialmente con las materias sensibles, tales como preferencias y

hábitos sexuales, actividades políticas y prácticas religiosas, en lugares privados y en públicos. **(El rincon del vago, 2004)**

Privacidad de Comunicación Personal

Los individuos demandan un interés de poder comunicarse entre sí mismos, usando varios medios, sin vigilar lo rutinario de sus comunicaciones por otras personas u organizaciones. **(El rincon del vago, 2004)**

Privacidad de Datos personales

Las personas que navegan o usuarios, emplazan que los datos sobre si mismos no deben estar automáticamente disponibles para otros individuos u organizaciones, y que, las bases de datos donde estos son almacenados, el individuo debe poder ejercitar un grado substancial de control referente a esos datos y su uso. **(El rincon del vago, 2004)**

Consideraciones en torno a la privacidad en las aplicaciones de Internet

La privacidad como configuración predeterminada

(Brian Nougrères, 2012, pág. 10) Partimos de la base de que lo primero que se genera son las configuraciones que han sido predeterminadas teniendo en cuenta la especial valoración del elemento privacidad.

(Brian Nougrères, 2012, pág. 10) El sistema se genera con total certidumbre, previendo desde el inicio la privacidad, razón por la cual no hay opción posible de que la configuración no preste a los elementos de protección del dato la debida atención y consideración ni es posible que el usuario del sistema pueda actuar con error aplicando un parámetro que contradiga los elementos básicos de la protección del dato personal.

Privacidad integrada en el diseño

(Brian Nougrères, 2012, págs. 10-11) El concepto de PbD se presenta integrado en el diseño y la arquitectura de los sistemas de tecnologías de la información y en las prácticas de negocios.

(Brian Nougrères, 2012, págs. 10-11) Lo referente a la protección de datos no está agregado al sistema, no está superpuesto al sistema ni es un anexo al mismo. Es un componente esencial del sistema: su núcleo funcional.

(Brian Nougrères, 2012, págs. 10-11) Se presenta holísticamente, esto es, abierto a los nuevos contextos que puedan surgir, como factor de integración e interacción de los distintos intereses involucrados y, además, en una forma por demás creativa, por cuanto se prevé la necesidad de autoinventarse a sí misma cuando no existan otras alternativas viables.

Respeto por la privacidad del usuario

La idea de PbD es mantener todo el sistema centrado en el usuario. Tanto los arquitectos como los operadores tienen la responsabilidad de proveerle de fuertes esquemas de privacidad por defecto, que recaben el previo consentimiento y fortalezcan las soluciones que son amigables para el usuario.

En general, se entiende que los mejores sistemas son los que han sido conscientemente diseñados con especial atención a las necesidades de los usuarios, que son los primeros interesados en manejar su propia información.

Otorgar al usuario la posibilidad de jugar un rol activo en la manipulación de sus propios datos puede constituir un chequeo muy efectivo contra malos usos y abusos de la protección de datos personales. Para ello, el usuario debe otorgar su consentimiento en forma libre y específica, y poder controlar la veracidad de la información, a cuyos efectos debe proveérsele de acceso a dicha información, así como de los medios de reclamo en casos de verificarse inexactitud en sus datos. Tanto las soluciones técnicas como las operaciones de negocios y las

arquitecturas físicas de las redes, en fin, todo el sistema debe proveer al usuario de un grado tal de consideración que lo coloque en el centro de las operaciones de acopio de datos personales. **(Brian Nougrères, 2012, págs. 10-11)**

Opiniones sobre la privacidad

El juez **(Miranda Alcántara, 2003, pág. 2)** señala: "la libertad informática implica tanto el derecho del individuo a negarse a brindar información sobre sí mismo y el derecho a pretender información concernida a su persona o personalidad; en suma controlar la identidad personal informática a través del consentimiento para preservar, acceder, o rectificar datos informativos referidos a la vida privada de las persona" en el mismo sentido refiere **(Miranda Alcántara, 2003, pág. 3)** "la libertad informática, el derecho a la intimidad cobra una dimensión mayor al buscar garantizar la intrusión no consentida sobre aspectos de la vida que uno reserva para sí y la información sobre la misma y que además debe proteger el desarrollo de la libertad personal."

Señala:

> *Por su parte, se ha de considerar que* ***las nociones de intimidad y de vida privada son difusas, no existe una definición de los conceptos que sea más o menos universal, así su contenido y márgenes ha de ser delimitado preferentemente por la autoridad judicial****. Al respecto, se ha de reconocer, que el desarrollo tecnológico ha implicado una ampliación del concepto, pues una visión restrictiva de la intimidad como un mero derecho subjetivo al secreto o al disfrute de la tranquilidad domiciliaria, se ha visto superado hoy tras la posibilidad de captar y reproducir escenas de la vida privada sin necesidad de saltar rejas o romper cadenas, v.g. mediante colocación de cámaras o micrófonos ocultos. Así pues, una versión expansiva considera a la intimidad como aquella parte de la vida de*

las personas donde tiene lugar la toma de decisiones personalísimas y se ponen las bases para la consecución de la autorrealización personal. La intimidad garantiza la autonomía individual, incluidas la libertad de elección sexual, y la titularidad individual sobre el propio cuerpo; garantiza la libertad de opción política y de disensión; y, garantiza las condiciones necesarias para la formación y elaboración de las opiniones públicas. **(Díaz Tolosa, 2007)**

El derecho a la intimidad garantiza a todo individuo un ámbito privado donde retirarse para reflexionar o actuar sobre decisiones vitales personalísimas. La intimidad es un último reducto donde el ciudadano puede ejercer la opción de ser diferente, donde se puede plantear estilos de vida o actitudes personales alternativas, lo cual, además implica el poder controlar la apropiación y divulgación de lo íntimo, pues se concibe como el derecho a mantener ámbitos de reserva de los que se excluye a otras personas **(Díaz Tolosa, 2007)**

G. La intimidad y su relación con la privacidad

En cuanto al derecho a la intimidad y la privacidad, existe una delgada línea que separa estos derechos, sin embargo, al abordarlos con mayor profundidad están intrínsecamente relacionados, veamos:

"En cuanto al derecho la intimidad, ***es aquel en el que se encuentran un núcleo de personas al que regularmente queremos proteger con un ánimo mucho mayor, por considerarlo inseparable de la esencia misma de nuestra propia vida y de la privacidad***" de tal forma que este derecho es aún más restringido que el señalado anteriormente: se relaciona directamente con nuestro círculo más cercano y con aquellos a los que por sobre todas las cosas deseamos proteger.

(s/a, conocimientosweb.net, 2013).

El Derecho a la vida privada (objeto de estudio del Derecho a la Intimidad), como Derecho autónomo tiene su punto de partida el año de 1890, ya que antes era incluido en otros Derechos. **(Basilio Araujo & Samamé Toribio, 2008, pág. 1)**

Otro nivel de análisis puede darse al abordar estos conceptos desde la perspectiva lingüística, pues intimidad y privacidad jurídicamente son dos derechos distintos, a lo que debe señalarse que ambos están intrínsecamente relacionados pues no se puede hablar de uno sin desligar al otro. Semánticamente o significativamente, ambos conceptos presentan una sinonimia entre sí, es decir se presenta una idea similar para ambos conceptos, por lo cual en el imaginario de las personas, los conceptos suponen una igualdad, veamos los significados que el diccionario Larousse señala:

Intimidad

1 Amistad y confianza profundas entre personas: nos vemos de vez en cuando y no tengo intimidad con él.

2 *Conjunto de pensamientos, sentimientos, sensaciones o hábitos propios de una persona, familia o grupo*: eso forma parte de mi intimidad y no voy a contarlo.

3 *Espacio doméstico y familiar en que se desenvuelve una persona o grupo*: añoro mucho la intimidad del hogar cuando estoy fuera.

4 Grupo de personas que comparten una relación de parentesco o gran amistad: la boda se celebró en la intimidad de la familia.

5 Partes sexuales del hombre o de la mujer: al final del programa, una chica exhibe sus intimidades.

Privacidad

Carácter de lo privado o íntimo: unos fotógrafos violaron la privacidad del artista.

Respecto a los dos términos analizados, nuestra legislación en la constitución política en cuanto a la intimidad, acoge literalmente la dimensión personal y familiar de la tercera acepción (*Espacio doméstico y*

familiar en que se desenvuelve una persona o grupo), sin embargo el concepto que desarrolla mejor las características que constituye la intimidad es el segundo (*Conjunto de pensamientos, sentimientos, sensaciones o hábitos propios de una persona, familia o grupo*), este es el concepto sobre el que giran tantas discusiones en la regulación de la red, pues las aplicaciones de internet se adueñan de informaciones que de acuerdo a la definición antes tratada es de carácter íntimo de la persona.

H. Diferencias entre privacidad e Intimidad

Dados los antecedentes expuestos, **(Vásquez Rocca, 2010)** la intimidad aparecería claramente delimitada como un derecho incuestionable, supremo e incomunicable, sin embargo, sigue siendo habitual que en el uso corriente y jurídico la distinción entre privacidad e intimidad se difumine con una extrema facilidad. De modo tal que se hace fundamental demarcar las distinciones entre uno y otro ámbito. Debe acotarse el léxico para dar situar la privacidad y la intimidad en el juego de lenguaje que constituye su lugar natural, cuestión que ha sido prolijamente examinada por José Luis Pardo en su texto La Intimidad, y sobre el cual se pretende esbozar algunas anotaciones y puntualizaciones exigidas por las transformaciones habidas lugar en el presente inicio de siglo en nuestras formas de vida y modos de organizar la convivencia.

El estudio de Pardo busca profundizar más allá de la perspectiva psicológica y sociológica, ámbitos en los que se había puesto el mayor énfasis. La analítica de Pardo en torno a la problematicidad del concepto de 'intimidad' comienza –precisamente– en este punto y lo hace a partir de delimitaciones fundamentales. Se señala por ejemplo que la intimidad "se trata de lo 'más recóndito e intrínseco de la persona' o 'lo más interno e inexpresable del hombre', una 'zona sagrada', 'lo más sagrado del hombre', 'lo más inefable', 'lo más interno del individuo', 'un ámbito casi inefable de la naturaleza humana', que 'toca las capas más profundas de

la persona', con 'un carácter en cierto modo sagrado', 'por su propia inexpresabilidad'". **(Vásquez Rocca, 2010)**

La palabra 'intimidad', que viene del latín intimus, ***superlativo de interior, designa cierto ámbito que se abre en lo que ya es interior***. Es un lenguaje simbólico para dar a entender la dimensión propiamente espiritual del alma humana, que va más allá de la vida puramente biológica.

En el hombre sin embargo la interioridad es particularmente desarrollada y compleja debido a su autoconciencia. Para referirnos a tal complejidad solemos hablar de "lo psicológico", ya que este es el objeto de la psicología y la psiquiatría. Pues bien, más allá de esta interioridad psicológica la vida humana presenta una dimensión única, que es inaccesible para la ciencia empírico-positiva porque no es un "grado" más de interioridad, sino un nuevo orden: el espiritual. En virtud del espíritu el hombre sabe y dispone de sí y es capaz de autoposeerse y autodestinarse; en una palabra, puede asumir la verdad última de su ser y decidir conforme a ella. La intimidad consiste precisamente en el ejercicio de esta libertad radical por la cual el hombre se hace fiel a sí mismo, al tiempo que se descubre inagotable, inabarcable, irreductible a las cosas.

En este sentido, el derecho a la privacidad comprende el derecho de la intimidad que tiene un carácter más estricto y dimensión individual que abarca como aspectos básicos la concepción religiosa e ideológica, la vida sexual, el estado de la salud, la intimidad corporal o pudor, entre otros.

Si partimos desde la perspectiva psicológica, sabemos que a diario escuchan en sus consultas intimidades de sus pacientes marcados por un tema contractual, yo te pago tú me escuchas. ¿Se puede llamar a esto intimidad? "sus ficheros (adecuadamente protegidos por el secreto

profesional) están repletos de incestos, violaciones, sueños eróticos, fantasías sadomasoquistas y confesiones vergonzosas del burgués en pantuflas o el proletario en el excusado...". Cotidianamente acostumbramos entender que esto podría manifestar su intimidad, aquello que hace, piensa o dice, cuando nadie lo ve, y que si lo publicara o se hiciera público, probablemente no podría volver a mirar a la cara a sus pares.

Un aporte importante en el tema de la Intimidad lo ha realizado Levinas visualizando y mostrándonos la necesidad del rostro, y en particular la mirada, es el principio de la conciencia emotiva, ya que la identidad sólo puede constituirse a partir de la mirada del otro; frente a ella develamos nuestra frágil desnudez, nos volvemos vulnerables y comprensibles, somos traspasados.

Avancemos hacia la distinción entre privacidad v/s intimidad lo que hemos expuesto y discutido hasta ahora no es nada menos y nada más que la privacidad, lo que las personas sueñan con hacer en privado, es esa la razón por la cual se la cuenta al psicólogo, con quienes se desahogan, lograr extraer de su núcleo esta especie de exterioridad que les tare paz, pero en ningún sentido se trata de una relación íntima. Incluso existen ocasiones en que este vínculo (psicólogo-paciente) está marcada por la desconfianza por un afán terapéutico de buscar el engaño del paciente, pues piensan que éstos no dirán la verdad sobre sí mismos.

Al delimitar el ámbito privado del público podemos distinguir dos tipos de acciones privadas, las internas y las externas. Las acciones privadas internas están constituidas por los comportamientos o conductas íntimas o inmanentes que principian y concluyen en el sujeto que los realiza, no trascendiendo de éste, comprendiendo los hechos o actos realizados en absoluta privacidad o de los que nadie puede percatarse.

Las acciones privadas externas son conductas o comportamientos que trascienden al sujeto que las realiza, siendo conocidas por los demás, pero que no afectan ni interesan al orden o la moral pública, ni causan perjuicios a terceros, vale decir, no afectan al bien común.

Ambas dimensiones conforman parte del derecho al respeto de la vida privada de las personas y su familia que el Estado debe asegurar, garantizar y promover, lo que las diferencia claramente de las acciones públicas.

En efecto, las acciones públicas son acciones externas que trascienden a quien las ejecuta y que -por ello- pueden afectar el orden o la moral pública o causar daños a terceros, por lo que el Estado pueda regularlas y, eventualmente, prohibirlas.

Asimismo se debe avanzar por eliminar aquellos prejuicios que están marcando el concepto de intimidad al definirla como "algo inexpresable e incomunicable, sin relación alguna con el lenguaje, y el sentido, que sólo se experimenta auténticamente (o supremamente) en soledad, cuando toda relación con otro está excluida". La falacia sostenida acerca de la intimidad expuesta recae en la idea de confundir intimidad con identidad (naturaleza humana). Aquí la intimidad se convertirá en una especie de ley que no podría romperse. Lo segundo es liar la intimidad con la propiedad privada, el derecho a la propiedad está garantizado por el Estado. Además la perspectiva que lleva a entenderla como limpieza étnica y, por último, el solipsismo, donde se presenta la intimidad como radicalmente incompartible y que sólo se puede experimentar en soledad.

Dejados estos prejuicios y ligazones respecto del concepto de intimidad, vayamos por su verdadera esencia que debe ser entendida como el saber en sí, la capacidad que el hombre pueda ensimismarse,

volverse, por así decirlo, de espaldas al mundo "no importa cuál sea el grado de falsedad o de falsificación social que uno arrastre consigo en su vida pública, en su intimidad se encuentra a sí mismo y atesora la verdad última y definitiva acerca de su ser".

Pero no debería ser de manera contraria, es decir, que uno no tuviese miedo a mostrarse de la manera en que 'se es' ¿por qué está prohibido (socialmente) el hecho de mostrarse o abrirse tal cual?, ¿es la intimidad algo anómala, amoral, que no se puede exhibir?. "¿es la intimidad un mal –una anomalía- que no revelo a los demás por temor a que rompan su asociación conmigo, o es un bien –lo que no nos obligaría a presuponer una naturaleza antisocial del hombre- que preservo de los demás porque yo mismo lo considero valioso y sé que sólo manteniéndolo en reserva puedo conservar su disfrute?".

Si la observamos como un bien, para compartirla elegimos a un invitado a participar de nuestros espacios "al confiarle su intimidad, le invita a compartir su silencio, a guardarlo junto con él. Ese silencio no puede revelarse a los otros, pero no porque esté prohibido –pues sólo lo que es posible puede prohibirse- sino porque es imposible, porque no hay palabras ni imágenes para hacerlo, únicamente puede compartirse en la intimidad, porque no hay más intimidad que la compartida: eso el ser compartida, sólo puede ser algo –sólo puede ser alguien- si se inclina por algo o por alguien". En este sentido, la intimidad no se devela sino que se destruye.

La intimidad, se devela, se nos muestra cuando comenzamos a evidencias nuestras interioridades, nuestras historias. Esta arte nos hace sensibles a los lectores puesto que nos muestra la trama de relaciones íntimas entre personas, no se trata de contarnos sólo la historia de los personas sino cuando ello transciende a quien lee, que se hagan

tangibles el pavor, el miedo, la alegría sin la necesidad de evidencias con palabras dichos sentimientos.

Por tanto, es necesario concebir y distinguir que la intimidad más que presentarse como una condición o propiciada por el lenguaje, aparece como efecto de él. Como sostiene Pardo sin intimidad podría existir lenguaje, sin embargo, pero nadie podría hablar, además de nadie querer utilizarlo.

Sin historia, sin fuerza interior el lenguaje no se podría vivenciar, tomar la fuerza y lograrse exteriorizar aquello que conforma el alma.

I. El derecho a la protección de datos personales

En nuestro país el mencionado derecho a proteger nuestros datos personales, es definido por **(Ministerio de Justicia y Derechos Humanos, 2014)** como: "**Los datos personales son cualquier información que permite identificar a una persona**. El nombre, los apellidos, la fecha de nacimiento, la dirección del domicilio, la dirección de correo electrónico, el número de teléfono, el número de RUC, el número de la placa del vehículo, la huella digital, el ADN, una imagen, el número del seguro social, etc. son datos que identifican a una persona, ya sea directa o indirectamente".

Conceptuando este derecho en palabras de **(Emparan Legaspi, 2012, pág. 6)**, en México "datos personales son "cualquier información concerniente a una persona física identificada o identificable". En España, se definen como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas o identificables"."

Continuando con la definición antes citada, añade respecto a la protección de datos **(Miranda Alcántara, 2003, pág. 3)** "la libertad informática que implica tanto el derecho del individuo a negarse a brindar

información sobre sí mismo y el derecho a pretender información concernida a su persona o personalidad; **en suma controlar la identidad personal informática a través del consentimiento para preservar, acceder, o rectificar datos informativos referidos a la vida privada de las persona…**

En ésta perspectiva de la libertad informática, el derecho a la intimidad cobra una dimensión mayor al buscar garantizar la intrusión no consentida sobre aspectos de la vida que uno reserva para sí y la información sobre la misma y que además debe proteger el desarrollo de la libertad personal".

Complementa lo expresado en el párrafo anterior, **(Miranda Alcántara, 2003, pág. 3)** "Ocurre que las personas en su vida cotidiana generan diferentes datos o información como sus viajes al interior o exterior, el uso de la tarjeta de crédito, movimientos de cuentas bancarias, Declaraciones Juradas ante instituciones públicas, solicitudes de ingreso o de trabajo ante instituciones públicas o privadas, los que ordenados y sistematizados por la computadora permiten obtener un perfil de comportamiento de la persona que vulnera la intimidad y la libertad de los individuos".

Ejemplificando la protección a la que se alude en este apartado, **(Miranda Alcántara, 2003, pág. 5)** presenta lo que sigue: "No obstante se requiere de precisiones normativas, sean constitucionales o legales y jurisprudenciales; en tanto el inciso 6 del artículo 2 de la Constitución se refiere a los servicios informáticos en general, que pueden ser de medios de comunicación social o de personas naturales o jurídicas distintas; adicionalmente porque el artículo 686 del Código Procesal Civil en su parte pertinente de medidas cautelares innovativas establece la protección del derecho a la intimidad, señalando que cuando la demanda pretenda el reconocimiento o restablecimiento del derecho a la intimidad

de la vida personal o familiar, puede el Juez dictar la medida que exija la naturaleza y circunstancias de la situación presentada; con lo cual puede implicar eventualmente que se dicte una medida cautelar en protección de la intimidad en forma anterior a su difusión cuando el afectado haya tenido conocimiento de la propalación de información o datos referidos a su vida personal o familiar sin su autorización, cuando el Código procesal civil señala la procedencia del reconocimiento del derecho a la intimidad".

(Miranda Alcántara, 2003, pág. 7) "Finalmente el TC[14], en su sentencia 292/2000, del 30 de Noviembre del 2000, ha reconocido la existencia de un nuevo derecho fundamental: el derecho a la protección de datos, que es distinto del derecho a la intimidad".

> ***Este derecho lo define como el poder de control de la persona sobre sus datos personales, sobre su uso y destino****. Es un poder de disposición permanente sobre todos los datos relacionados con la persona, que deben ser protegidos en su ejercicio, de forma que cualquier persona tenga capacidad de control sobre los mismos y sepa, en todo momento, quiénes tienen sus datos, con qué finalidades y pueda negarse a facilitarlos o bien modificarlos, pues de los contrario, este nuevo derecho quedaría vacío de contenido. El derecho a la intimidad personal y familiar y el derecho a la protección de datos,* ***aún siendo distintos tienen una base común: la dignidad de la persona humana y los derechos inviolables que le son inherentes*** **(Miranda Alcántara, 2003, pág. 7)**.

Uno de los temas más a tener en consideración dentro de protección de datos o contenidos personales es su permanencia en la red, **(Alonso, 2011, pág. 7)** "En líneas generales, lo que se publica en internet permanece. Cuando escribes algo en internet y lo publicas en una página de libre acceso debes asumir que esas líneas van a quedar permanentemente almacenadas y disponibles en esa página. Puede que no siempre sea así, pero es lo más habitual. Es la hipótesis con la que se

[14] *Tribunal constitucional*

debe trabajar online. En primer lugar no siempre controlas el servicio en el que estás dejando tu opinión. Es más, lo habitual es que no lo hagas, que se trate de un servicio controlado por un tercero que **no siempre va a estar dispuesto a darle curso a tu petición de retirar determinados contenidos**."

Por otro lado la cultura que predomina en el ciber espacio, es la idea del "copy and paste" o coloquialmente conocido como "Copia y pega", a lo cual explica detalladamente **(Alonso, 2011, pág. 7)** "...hay que ser consciente de que el mecanismo fundamental de difusión de la información en internet es la copia. **En cuanto algo se publica empieza a ser replicado múltiples veces. Desde la caché de Google a las copias de otros servicios, el Internet Archive o los pantallazos que capturan los propios internautas**. Incluso si la publicación original de la información se hizo en privado, la facilidad de copia unida a un número suficientemente alto de usuarios con acceso a ella y a conexiones entre ellos no suficientemente fuertes, hace que las probabilidades de que se haga pública sean muy altas. Y eso sin contar con posibles fallos técnicos o humanos que también pueden revelarlas. Parafraseando a Linus Torvald: **dado un número suficientemente alto de ojos, cualquier información que publiques en internet estará permanentemente disponible**."

La facilidad para encontrar algún contenido o información sea personal o no, se ha vuelto cotidiana y habitual, tal como amplía **(Alonso, 2011, pág. 7)** "**Cualquier contenido publicado en internet en una página abierta es susceptible de ser localizado, indexado, copiado y enlazado por Google**. Una vez que esto sucede, está al alcance de una simple búsqueda. No es tanto que se publiquen cosas que antes no estuvieran publicadas. Es que Google hace insultantemente sencillo acceder rápidamente a ellas. Si has sido condenado alguna vez, o has dejado de pagar el alquiler un mes, o te han embargado alguna vez, dicha

información constaba en registros públicos. Pero tenías que ir a consultarlos. Y encontrarla. Era un proceso tedioso, complicado y que no siempre tenía éxito. Ahora esa misma información se encuentra con una mera búsqueda en menos de veinte segundos. Si el usuario sabe lo que busca, casi siempre lo va a encontrar. Y a veces también sin saber a priori que lo buscaba."

En el ámbito Europeo, **(Piñar Mañas, 2005, pág. 3)** establece que: "La Constitución Europea reconoce en dos ocasiones el derecho fundamental a la protección de datos. Asimismo establece que todos los países miembros de la Unión Europea deberán contar con una autoridad independiente que garantice y tutele tal derecho. La Ley Orgánica 15/1999 regula el derecho fundamental a la protección de datos y dispone que será la Agencia Española de Protección de Datos la encargada de tutelar y garantizar el derecho".

i. ¿En qué consisten los datos personales?

Mínimamente según **(Piñar Mañas, 2005, pág. 7)** **"**Los datos personales permiten identificar a una persona**"**.

Extendiendo un poco el concepto se puede detallar:

"El nombre, los apellidos, la fecha de nacimiento, la dirección postal o la dirección de correo electrónico, el número de teléfono, el número de identificación fiscal, el número de matrícula del coche, la huella digital, el ADN, una fotografía, el número de seguridad social, ... son datos que identifican a una persona, ya sea directa o indirectamente".

En cuanto a cómo se recogen estos datos personales detalla **(Piñar Mañas, 2005, pág. 7)** "Es habitual que prácticamente para cualquier actividad sea necesario que los datos personales se recojan y utilicen en la vida cotidiana. Una persona facilita sus datos personales

cuando abre una cuenta en el banco, cuando se matricula en un curso de idiomas, cuando se apunta al gimnasio, cuando solicita participar en un concurso, cuando reserva un vuelo o un hotel, cuando pide hora para una consulta médica, cuando busca trabajo, cada vez que efectúa un pago con su tarjeta de crédito, **cuando navega por Internet**... Son múltiples los rastros de datos que se dejan a menudo en todas estas gestiones. Los mecanismos de recogida y tratamientos de los datos personales se encuentran en constante evolución.

Desarrollando la idea anterior **(Piñar Mañas, 2005, pág. 8)** señala: "Ello supone que el desarrollo y la aplicación de las nuevas tecnologías han introducido comodidad y rapidez en el intercambio de datos, lo que ha contribuido también al incremento del número de tratamientos de datos que se realizan cotidianamente. La bondad que aportan estas técnicas es indudable respecto del progreso de las sociedades modernas y de la calidad de vida de los ciudadanos, **pero se hace necesario garantizar el equilibrio entre modernización y garantía de los derechos de los ciudadanos**. **Esta ponderación entre derecho del ciudadano a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la Información, es el contexto en el que el Legislador consagra el derecho fundamental a la protección de datos de carácter personal"**.

El tratadista peruano detalla con precisión al respecto **(Orrego, 2014, pág. 1) El derecho de autodeterminación informativa o protección de datos personales**, es de reciente recepción en el ordenamiento constitucional peruano, a través del artículo 2o, inciso 6º. Este derecho fundamental ha merecido una complementación interesante por medio de dos fuentes del derecho jurídicas: el Código Procesal Constitucional y la Jurisprudencia Constitucional.

ii. Contenido y restricciones del derecho a la protección de datos

El profesor en Derecho Constitucional de la Pontificia Universidad Católica del Perú y la Universidad Nacional Mayor de San Marcos realiza un análisis amplio de la norma que fue promulgada el 3 de julio del 2011 y que lleva por denominación "Ley de protección de datos personales", veamos **(Huerta Guerrero, 2012)** "La norma es extensa, algo confusa en su redacción y con un orden en el desarrollo de los temas que puede perjudicar su adecuada comprensión por parte de la ciudadanía en general, que viene a ser su principal destinatario. Por ello, en el presente blog deseamos explicar los aspectos más importantes de esta Ley, siguiendo el orden empleado cuando se estudian los derechos fundamentales reconocidos en la Constitución".

iii. Aspectos generales de la ley de protección de datos personales

En alusión a ley de protección de datos personales, resume el contenido muy brevemente **(Huerta Guerrero, 2012) "La Constitución de 1993 contiene una redacción deficiente sobre los alcances de este derecho, que se limita a reconocer solo la facultad de toda persona a evitar que se suministre a terceros información que pueda afectar su intimidad personal o familiar**. En este sentido, el artículo 2º inciso 6º del texto constitucional señala que toda persona tiene derecho:

"A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar**"**.

Complementando los señalado líneas arriba, **(Huerta Guerrero, 2012)** señala. "Una mejor precisión sobre el contenido del derecho se encuentra en el Código Procesal Constitucional (artículo 61º inciso 2º) y la jurisprudencia del Tribunal Constitucional. En el caso del Código se señala que el proceso de hábeas data protege el derecho de toda persona a:

"*Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales*".

Adentrándonos al corpus propio de la ley **(Huerta Guerrero, 2012)** explica: "En la nueva Ley, entre los artículos 18º a 23º, se precisan con mayor detalle los derechos del titular de datos personales, como el de información sobre el tratamiento que se dará a los datos, de acceso a las bases respectivas, de actualización, inclusión, rectificación y supresión de datos, a impedir su suministro a terceros y de oposición. Sin embargo, **llama la atención que respecto de la mayoría de estos derechos se haya previsto (en el artículo 26º) el abono de una contraprestación, cuando en experiencias comparadas, al menos en el caso del acceso, rectificación, cancelación y oposición, no se exige pago alguno. Se trata de una medida que podría desincentivar el ejercicio de alguno de estos derechos**.

Otro punto importante a considerar se encuentra referido a los "sujetos pasivos" dentro de la conocida ley de protección de datos personales, donde **(Huerta Guerrero, 2012)**, analiza:

"Nos referimos a los sujetos que se encuentran obligados a realizar alguna actividad concreta a favor de este derecho. En este sentido, la Ley dispone que **los sujetos pasivos del mismo son los titulares y encargados de bancos de datos personales de administración pública y de administración privada (art. 3), exceptuándose los bancos de datos privados creados para uso privado y los bancos de datos de la administración pública destinados al cumplimiento de las competencias de las entidades públicas o para la defensa nacional,**

la seguridad pública y la investigación penal. Las obligaciones específicas para los titulares y responsables de los bancos de datos se precisan en el artículo 28º de la Ley. Las infracciones respectivas por incumplir tales obligaciones, así como las sanciones aplicables, se encuentran previstas en el Título VII (artículos 37º al 40º).

Se debe prestar especial atención al tema de las garantías sustanciales propuestas por la ley referida anteriormente y en atención a ello **(Huerta Guerrero, 2012)** desataca: "**La garantía más importante en materia de datos personales está referida al tema del consentimiento** para el tratamiento de los mismos. En este sentido, el artículo 13º de la Ley señala que **los datos personales sólo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto**. Precisa asimismo que **el consentimiento debe ser previo, informado, expreso e inequívoco.** Además, en su artículo 14º establece aquellos casos en donde no resulta necesario el consentimiento. La norma también ha previsto (artículo 17º) **el deber de confidencialidad respecto a los datos personales por parte de los titulares de los bancos de datos, los responsables del mismo y del personal que interviene en cualquier etapa de su tratamiento**.

Debe anotarse que lo dicho anteriormente en relación al Marco civil brasileño, se encuentra muy por debajo de lo que debiere proteger, puesto que no solo se debe tener en cuenta el consentimiento, sino como lo señala la legislación brasileña, debe prestarse un apartado especial sobre el punto que concierne al consentimiento, pues este debe ser expreso y puesto en un apartado diferente a todas las demás condiciones que plantean las aplicaciones de internet, de otro lado las garantías propuestas por la ley en su mayor parte son universales y equívocas, debido a que regulan aspectos generales de lo que deben proteger de un usuario.

La ley bajo análisis, plantea límites para ejercer el derecho a proteger sus datos personales, que como acabaremos viendo no persigue proteger al ciudadano sino a otros intereses, por lo que en relación al marco brasileño deja mucho que desear, veamos lo que rescata **(Huerta Guerrero, 2012)** "El derecho a la protección de datos no es absoluto y admite restricciones. En este sentido, el artículo 27º de la Ley señala que el ejercicio de **las facultades de acceso, supresión y oposición pueden ser limitados a fin de proteger derechos e intereses de terceros**, o cuando se puedan ver obstaculizadas actuaciones judiciales o administrativas en curso, vinculadas al cumplimiento de obligaciones tributarias o previsionales, investigaciones penales, desarrollo de actividades de control de la salud y del medio ambiente, verificación de infracciones administrativas u otros supuestos que establezca la ley. **El mencionado artículo señala que estas limitaciones operan respecto a las bases de datos de la administración pública.**"

En cuanto a las vías de actuación para defender el derecho, **(Huerta Guerrero, 2012)** explica: "El artículo 24º de la Ley **reconoce la protección del derecho a través de una vía administrativa, que se sigue ante la Autoridad Nacional de Protección de Datos Personales** conforme al procedimiento previsto en los artículos 219º y siguientes de la Ley del Procedimiento Administrativo General (Ley Nº 27444). Contra lo resuelto por la Autoridad Nacional cabe iniciar un proceso contencioso-administrativo. A la vez, la Ley reconoce la posibilidad de acudir de forma directa al proceso constitucional de hábeas data. De acuerdo con la Sexta Disposición Complementaria Final, **el procedimiento administrativo previsto en el citado artículo 24º no debe ser entendido como una vía previa para acudir al hábeas data**. Conforme se aplique la norma se podrá evaluar cuál de estas alternativas será la más empleada por las personas que consideren afectados sus derechos".

En cuanto a la plena activación de la ley **(Huerta Guerrero, 2012)** sostiene para su momento: "Sólo algunas disposiciones de la Ley han entrado en vigencia, como **las referidas al procedimiento de implementación de la norma y el Título II, que reconoce la garantía del consentimiento del titular para el tratamiento de sus datos personales**, las excepciones a este consentimiento, el deber de confidencialidad por parte de quienes son responsables del tratamiento de datos, entre otros aspectos. En consecuencia, el resto de disposiciones sólo entrará en vigencia a partir de la expedición del Reglamento respectivo, que deberá ser emitido en un plazo no mayor de 120 días hábiles contados a partir de la instalación de una Comisión Multisectorial responsable de su elaboración, que a su vez debe ser instalada en un plazo máximo de 15 días a partir del día siguiente de la publicación de la Ley. **Sin embargo, a pesar que la Ley no señala la vigencia de los artículos referidos al contenido del derecho, ello no impide su ejercicio, así como la respectiva protección judicial, *en tanto los derechos fundamentales no están condicionados –en cuanto a dicho ejercicio y protección- a la existencia o vigencia de una ley***, como se acredita con la jurisprudencia constitucional emitida hasta el momento por el Tribunal Constitucional.

Finalmente y a modo conclusivo, presentamos lo señalado por **(Huerta Guerrero, 2012)**, en lo que considera las reflexiones finales de la ley de protección de datos personales.

La aprobación de la Ley de Protección de Datos Personales constituye una medida acertada por parte del actual Congreso de la República, cuyo período legislativo está a punto de culminar. Corresponderá al próximo Congreso realizar las modificaciones que sean necesarias, conforme se vaya aplicando la norma. Además, será de su competencia aprobar las modificaciones legales que sean necesarias para adecuar la legislación existente al texto de la nueva Ley aprobada,

conforme se dispone en su Cuarta Disposición Complementaria **(Huerta Guerrero, 2012)**.

En el caso del Poder Ejecutivo ocurre algo similar, pues corresponderá al próximo Gobierno, que inicia sus funciones el 28 de julio del 2011, dictar el Reglamento respectivo e implementar el funcionamiento de la Autoridad Nacional de Protección de Datos Personales, cuyas competencias son bastante numerosas (artículo 33º de la Ley) y que deberá tener oficinas en todo el país, a fin de no concentrar en la capital la protección administrativa referida al tratamiento de datos personales **(Huerta Guerrero, 2012)**.

En cuanto a la jurisprudencia, corresponde al Poder Judicial y al Tribunal Constitucional garantizar el adecuado ejercicio del derecho así como la estricta observancia de todas las obligaciones que la Ley ha previsto para los titulares y responsables de las bases de datos. De modo particular, es probable que el Tribunal tenga que analizar la constitucionalidad de algunas de las normas contenidas en la Ley, como por ejemplo, la referida al abono de una contraprestación para el ejercicio de determinadas facultades que forman parte del contenido del derecho **(Huerta Guerrero, 2012)**.

iv. La iniciativa de Brasil y su posición en la protección de datos

Es de conocimiento, que el 2014 fue históricamente el que trajo más cambios a Internet y su regulación, Brasil en su normativa destaca la neutralidad "el responsable de la transmisión, conmutación o ruteo tiene el deber de tratar de forma isonómica cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación". **(Doneda, 2014)** "La discriminación o degradación del tráfico será reglamentada en los términos de las atribuciones privativas del Presidente de la República previstas en el inciso IV del artículo 84 de la Constitución

Federal, para la ejecución fiel de esta Ley, el Comité Gestor de Internet y la Agencia Nacional de Telecomunicaciones":

El manejo de Internet en Brasil cuenta con los siguientes principios:

- Protección de la privacidad;
- Protección de los datos personales, en forma de ley;

En cuanto a los derechos y garantías de los usuarios **(Doneda, 2014)** Brasil establece que el acceso a internet es esencial para el usuario y el ejercicio de la ciudadanía están garantizados los siguientes derechos:

I. *La inviolabilidad de la intimidad y de la vida privada, asegurando el derecho a su protección y a la indemnización por el daño material o moral* resultante de su violación;
II. *La inviolabilidad del flujo y secreto de las comunicaciones* por Internet, salvo por orden judicial, de acuerdo con la ley;
III. *La inviolabilidad y el secreto de sus comunicaciones privadas* almacenadas, salvo por orden judicial;
IV. *La imposibilidad de suministrar a terceros sus datos personales*, incluyendo registros de conexión y acceso a aplicaciones en Internet, salvo mediante consentimiento libre, expreso e informado o en circunstancias establecidas por la ley;
V. *El consentimiento expreso sobre la recogida, uso, almacenamiento y tratamiento de datos personales*, que deberá presentarse de forma destacada de las demás cláusulas contractuales;
VI. *La información clara y completa sobre la recogida*, uso, almacenamiento, tratamiento y protección de sus datos personales, que sólo podrán ser utilizados para finalidades que:
    a) justifiquen su recolección;
    b) no estén prohibidas por ley; y

c) queden especificadas en los contratos de prestación de servicios o en los términos de uso de las aplicaciones de Internet.

VII. *El borrado definitivo de los datos personales* que se hayan proporcionado a determinada aplicación de Internet, a solicitud suya, al término de la relación entre las partes, salvo en los casos de custodia obligatoria de registros previstas en esta ley;

Además es regla que "La garantía del derecho a la privacidad y a la libertad de expresión en las comunicaciones es condición para el pleno ejercicio del derecho de acceso a Internet". **(Doneda, 2014)**

(Doneda, 2014) "*Son nulas las cláusulas contractuales que violen lo anterior y las que impliquen ofensa a la inviolabilidad y al secreto de las comunicaciones privadas a través de Internet*"; en nuestro país, existe una norma de protección de datos personales, sin embargo, el legislador deja sin protección al usuario al tocar este apartado.

En cuanto al guardado y registro de los datos de los usuarios en Brasil, **(Doneda, 2014)** señala "En la provisión de conectividad a Internet, cabe al administrador del sistema autónomo respectivo el deber de mantener los registros de conexión, bajo secreto, en un ambiente controlado y seguro, durante el plazo de un año, según el reglamento".

Lo más importante de los señalado **(Doneda, 2014)** "En la provisión de conexión, onerosa o gratuita, está prohibido almacenar registros de acceso a aplicaciones de Internet".

En la provisión de conexión, onerosa o gratuita, está prohibida la custodia: "de datos personales que sean excesivos en relación a la finalidad para la cual fue dado el consentimiento por su titular". **(Doneda, 2014)**

v. La protección de datos personales en el marco europeo

(Piñar Mañas, 2005, pág. 10) explica referente al marco Europeo: "La Constitución Europea ha recogido expresamente el derecho fundamental a la protección de datos en dos ocasiones, en la Parte I, Título VI (De la vida democrática de la Unión), el artículo I-51 (Protección de datos de carácter personal) establece en el epígrafe primero que "**toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan**" y en la Parte II (Carta de los Derechos Fundamentales de la Unión), Título II (Libertades), se introduce en el artículo II-68 la segunda referencia al derecho a la protección de datos, señalando de nuevo que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan", y añadiendo que "**estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley**", y que "toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación".

Respecto a quien se encargará de velar los derechos bajo el marco Europeo **(Piñar Mañas, 2005, pág. 10)** explica: "Asimismo, en ambos preceptos se establece que una autoridad independiente se encargará de la garantía del derecho fundamental a la protección de datos personales. **La Constitución Europea exige que en todos los Estados miembros exista una autoridad independiente que controle y garantice el Derecho Fundamental a la protección de datos**.

J. Límites de la protección de datos personales

i. La obtención de datos: el consentimiento

Para obtener datos se deben cumplir una serie de requisitos, de ellos se requiere que sea libre, informado, previo, expreso e inequívoco sin embargo aunque pareciere que se cubren casi todos los aspectos que deben tener real importancia respecto al consentimiento, un detalle a

considerar es que al referirse con el término de "expreso e inequívoco", se debería referir a que está totalmente entendido por la persona sin poder dar lugar a dudas o errores, sin embargo como se verá más adelante todo esto se subsume en un "clic" ¿se cumplirá realmente con ser expreso e inequívoco?; desarrollando los requisitos del consentimiento el **(Ministerio de Justicia y Derechos Humanos, 2014, pág. 10)**, señala:

Libre: Debe ser dado de manera voluntaria.

Previo: Pedido con anterioridad a la recopilación de los datos.

Expreso e inequívoco: Debe ser manifestado en condiciones que no admitan dudas de su otorgamiento.

La condición de expreso no se limita a la manifestación verbal o escrita tradicional. **Tratándose del entorno digital, también se considera expresa la manifestación consistente en "hacer clic"**.

Informado: Cuando al titular de los datos se le comunique de manera clara, expresa, con lenguaje sencillo quién, por qué, para qué y cómo van a ser tratados sus datos personales."

La ley tiene orientaciones positivas, de ellas **(Ministerio de Justicia y Derechos Humanos, 2014, pág. 11)**, "**Tu información personal te pertenece. Por tanto, si tienes el derecho de consentir su uso, también tienes el derecho de retirar ese consentimiento en cualquier momento**. Puedes revocar tu consentimiento para el tratamiento de tus datos personales para todas las finalidades que hayas consentido o solo para alguna de ellas. Es necesario que precises esto al momento de presentar tu solicitud ante el titular del banco de datos personales."

ii. Los derechos del usuario

Todo usuario en Internet debe contar con unos derechos mínimos que garanticen sus derechos, ello garantizado por la ley de Protección de Datos Personales, veamos:

Derecho a acceder

Toda persona tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

"Entre la información a la que el titular de los datos puede acceder se encuentra la siguiente: **(Ministerio de Justicia y Derechos Humanos, 2014, págs. 14-15)**

¿Cuáles de sus datos personales están utilizando?

¿Cómo fueron recopilados sus datos personales?

¿Para qué finalidades se recopilaron?

¿A solicitud de quién se realizó la recopilación?

¿Con quiénes comparten la información personal y para qué fines?

¿Qué transferencias de sus datos personales se realizan?

¿En qué condiciones están siendo tratados los datos personales?

¿Cuánto tiempo se conservarán sus datos personales?

El titular de los datos podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta implementados por el banco de datos personales:

- Visualización en sitio;
- Escrito, copia, fotocopia o facsímil;
- Trasmisión electrónica; o
- Cualquier otra forma idónea para tal fin.
- Cualquiera sea la forma a emplear, el acceso debe ser en formato claro, comprensible al conocimiento medio de la población.

Si la solicitud fuera estimada y el titular del banco de datos o encargado del tratamiento no acompañase a su respuesta la información solicitada, el acceso será efectivo dentro de los diez (10) días siguientes a dicha respuesta.

El tiempo para atender este derecho es de veinte (20) días.

El derecho de acceso ***permite saber qué datos se tiene sobre una persona para que pueda controlar la exactitud de los datos***, y en caso de ser necesario, hacerlos rectificar o cancelar.

Derecho de, actualizar, incluir, corregir o rectificar

Es el derecho del titular de datos personales que se modifiquen los datos que resulten ser parcial o totalmente inexactos, incompletos, erróneos o falsos.

Expandiendo lo relatado líneas arriba, **(Ministerio de Justicia y Derechos Humanos, 2014, pág. 16)**, "A través del ejercicio del derecho de rectificación el titular de los datos personales puede solicitar al titular del banco de datos o encargado del tratamiento que modifique los datos personales que resulten ser inexactos, erróneos o falsos.

A través del ejercicio del derecho de inclusión o actualización el titular de los datos personales podrá solicitar al titular del banco de datos personales que corrija los datos incompletos.

La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que deba de realizarse y deberá ir acompañada de la documentación que acredite lo solicitado.

De no acompañarse la información necesaria para proceder a la rectificación, el titular del banco de datos podrá requerir dentro de los siete

(7) días siguientes de recibida la solicitud, documentación adicional al titular de los datos personales.

El titular del banco de datos o responsable resolverá el pedido de rectificación en el plazo de diez (10) días hábiles. Si los datos personales hubieran sido transferidos previamente, el titular o encargado del banco de datos deberán comunicar la rectificación, actualización e inclusión efectuada a quienes haya transferido los datos, para que en el mismo plazo proceda a rectificar, actualizar o incluir según corresponda. El plazo para atender este derecho es de diez (10) días.

Derecho a cancelar

El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos personales de un banco de datos personales cuando éstos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recopilados; hubiere vencido el plazo establecido para su tratamiento; se ha revocado su consentimiento para el tratamiento y en los demás casos en los que no están siendo tratados conforme a la Ley y al reglamento.

(Ministerio de Justicia y Derechos Humanos, 2014, págs. 18-19), "Este derecho permite al titular del dato personal solicitar que se supriman, es decir se eliminen, sus datos personales materia de tratamiento cuando:

- Advierta omisión, error o falsedad.
- Cuando hayan dejado de ser necesarios, para la finalidad para la cual fueron recopilados.
- Cuando haya vencido el plazo establecido para su tratamiento.

Considere que no están siendo utilizados conforme a las obligaciones que tiene el titular y encargado del banco de datos

personales de acuerdo a lo establecido en el artículo 28 de la Ley de Protección de Datos Personales.

La cancelación no siempre va a proceder de manera inmediata. Durante el proceso previo a la cancelación, **el encargado del banco de datos va a disponer el bloqueo de los datos personales que consiste en impedir que terceros puedan acceder a ellos para utilizarlos**. Tal bloqueo no se aplica a las entidades públicas que requieran de la información para el adecuado ejercicio de sus competencias, por ejemplo el poder judicial, la administración tributaria.

Es importante tener presente que no siempre procederá la cancelación de tu información personal. En particular, los datos personales no podrán ser eliminados:

- Cuando deban ser conservados en virtud de razones históricas, estadísticas o científicas.
- Cuando sean necesarios para el desarrollo y cumplimiento de una relación contractual.
- Cuando deban ser tratados en virtud de una ley.

De lo visto anteriormente, no se expresa el hecho del borrado físico de las bases de datos de la información que se pretende cancelar, con lo cual no se defiende a la persona pues se velan intereses de la empresa en cuyos servidores están mis datos para que los revisen cuando ellos lo deseen, a lo cual tristemente no se le da la debida importancia ya que en realidad no se cancelan, suprimen o eliminen los datos sino solo se bloquea el acceso a terceros, que pasa si no se cumple con los requisitos para cancelar la información por omisión error o falsedad, no podría cancelarlos, quien delimita la utilidad delos datos recopilados para cancelarlos, por último, si dichos datos personales son parte de una relación contractual con una empresa digital en Internet, pierdo mi derecho a cancelar los datos, por que acepte expresa e inequívocamente

con "un clic", hay muchos aspectos de nuestra ley que dejan mucho que desear en relación al marco brasileño"

Derecho de oposición

Toda persona tiene la posibilidad de oponerse, por un motivo legítimo y fundado, referido a una situación personal concreta, a figurar en un banco de datos o al tratamiento de sus datos personales, siempre que por una ley no se disponga lo contrario.

iii. Códigos de conducta

Respecto al tema que se está abordando, se presentarán diferentes definiciones de las cuales en primer lugar, **(dellacasacastillo.com, 2014) "**Código de conducta: **declaración formal de los valores y prácticas comerciales de una empresa y, algunas veces, de sus proveedores**. Un código enuncia normas mínimas y el compromiso de la empresa de cumplirlas y de exigir su cumplimiento a sus contratistas, subcontratistas, proveedores y concesionarios. Fuente: Comisión de las Comunidades Europeas: "Libro Verde: fomentar un marco europeo para la responsabilidad social de las empresas" Bruselas, 2001**"**

Otra definición la propone **(derecho.com, 2014) "Conjunto de normas** no impuestas por disposiciones legales, reglamentarias o administrativas de un Estado miembro**, en el que se define el comportamiento de aquellos comerciantes que se comprometen a cumplir el código en relación con una o más prácticas comerciales o sectores económicos concretos.** El responsable de dicho código será aquella persona o entidad responsable de la elaboración y revisión de un código de conducta y/o de revisar su cumplimiento por quienes se hayan comprometido a respetarlo. **"**

Un aspecto a rescatar en relación al tema que se está emprendiendo es el referente a la conducta de los usuarios respecto a las aplicaciones en Internet, de lo cual amparándonos en lo establecido por la ley de Protección de Datos Personales, tendríamos todos los derechos que resguardan a los usuarios detallados algunos parágrafos atrás, sin embargo, para ejercerlos hay una serie de requisitos que la persona debe cumplir, a lo que explica el **(Ministerio de Justicia y Derechos Humanos, 2014, pág. 13)**, "**La persona debe dirigirse directamente ante el titular del banco de datos, acreditando su identidad y presentando copia del Documento Nacional de Identidad o documento equivalente**."

Resulta asertiva la decisión de la norma al regular este aspecto, sin embargo una persona ¿podrá acercarse a las oficinas de Google para recuperar su cuenta electrónica?, existe alguna en Perú ¿Esta acción estará amparada por la ley en defensa de sus datos personales? ¿Qué hay de su información íntima y sensible que se halla en la base de datos de esta empresa? ¿Cómo pretender la titularidad de una cuenta que no ha sido inscrita con mis datos reales? A pesar de estar protegido por una ley la práctica y ejercicio de los derechos protegidos no es posible, de otro lado no se es posible controlar los datos que me pertenecen si los términos de servicio cambian constantemente en detrimento de mi estabilidad jurídica.

iv. Contratos-Acuerdos

Atendiendo este tema se puede expresar **(Ministerio de Justicia y Derechos Humanos, 2014, pág. 9)** "Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, ***el derecho de información puede cumplirse mediante la publicación de políticas de privacidad***, las que deben ser fácilmente accesibles e identificables"

Y qué pasa si en estas comunicaciones se cambian los términos del acuerdo sin el consentimiento del usuario o se le notifican sin otra opción posible, ¿qué defiende la estabilidad jurídica del usuario respecto a su intimidad?

K. Relación del derecho a la Intimidad y de los datos personales

Refiere y reflexiona al abordar el tema sobre la privacidad de los datos personales el profesor de derecho empresarial y comercial **(Miranda Alcántara, 2003, pág. 3)** los que sigue: "La regulación de las nuevas tecnologías de la información y la comunicación en sí conlleva a la necesidad de **reflexionar sobre la función del derecho para proteger la intimidad o vida privada así como la identidad de las personas,** como garantía de un desarrollo libre y digno de la personalidad; estando al conflicto permanente entre el derecho a la información en su aspecto de libertad de información y el derecho a la vida privada o intimidad, último derecho que con el desarrollo de la informática se ha considerado que su protección se constituye como garantía de la libertad personal"

Dentro de lo que se consideraría como excepciones al derecho de acceso a la información esta, aquellas informaciones que afecten la Intimidad personal, al respecto señala: **(La Constitución Comentada, 2005, pág. 118)**, "El derecho de acceso a la información pública no es absoluto. De acuerdo con el artículo 2 inciso 5) de la Constitución, **las excepciones a su ejercicio pueden estar referidas a informaciones que afectan la intimidad personal**, la seguridad nacional y las que expresamente se excluyen por ley..."

Un punto importante a desarrollar se refiere a la distinción entre Intimidad y privacidad que como se verá está atendida en los siguientes términos **(La Constitución Comentada, 2005, pág. 123)**"...el marco doctrinario y la regulación legal en el Perú referente a la privacidad

económica, estableciendo sus límites, así como los mecanismos de seguridad que debe garantizar el poseedor de la información económica proveniente de la actividad bancaria o tributaria; precisando, además, que el secreto bancario y la reserva tributaria no forman parte de la intimidad de la persona sino de su privacidad económica, pues la intimidad corresponde al núcleo duro de los derechos fundamentales, por lo que goza de una protección mayor y su limitación es en extremo excepcional." De lo anteriormente señalado se puede deducir que la intimidad personal es mucho más preponderante, literalmente hablando, *goza de una mayor protección*, lo que no se ve reflejado en la realidad, pues no está mayor atendida que la privacidad económica y no se le considera superior.

Una diferencia importante la expresa **(La Constitución Comentada, 2005, pág. 124)**, señalando: "*la intimidad y la privacidad son libertades personalísimas, pero que están diferenciadas por lo que representan y por el grado de protección que el Derecho les confiere*"

Desarrollando la idea anterior, **(La Constitución Comentada, 2005, pág. 124)** explica: "...modernamente la privacidad y en especial la intimidad se vuelven derechos fundamentales en la medida en que se convierten para el hombre en bienes que representan estados deseables, como expresa Habermas: un ámbito de libertad frente a la despiadada colonización del mundo de la vida."

Un aspecto a tomar en consideración, los señala **(Emparan Legaspi, 2012, pág. 5)**, "El concepto de intimidad, sin embargo, se ha modificado, dice Aristeo García. En la actualidad, **la relevancia de la privacidad no está en que los demás no posean información sobre nuestra vida privada, sino en el derecho a decidir sobre el tratamiento que se le da a nuestros "datos personales**"."

"Ahora, con el tratamiento, la recolección, el almacenamiento de informaciones que antes sólo podía formar parte de la vida íntima de cada ser humano —o bien, era conocido por un mínimo sector—, ha ido variando paulatinamente su entorno y estructura. Esto es, los datos personales de toda persona se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados. Es por ello que el derecho a la intimidad ha tenido que ir redireccionando su ámbito de protección, donde además de la facultad del individuo de rechazar invasiones a su ámbito privado, ahora supone el reconocimiento de un derecho de control y acceso de sus informaciones, es decir, de toda aquella información relativa a su persona.(García, 2007, p. 745)" **(Emparan Legaspi, 2012, pág. 5)**.

2.2.4 BASES TECNOLÓGICAS

A. Tecnologías de Información y comunicación

Las Tecnologías de la Información y la Comunicación, también conocidas como TIC, ***son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro***. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes. **(s/a, Servicios TIC)**

Las TICs pueden ser clasificadas en dos sentidos: "Como las tecnologías tradicionales de la comunicación, constituidas principalmente por la radio, la televisión y la telefonía convencional, y por las tecnologías modernas de la información caracterizadas por la digitalización de las tecnologías de registros de contenidos como la informática, de las comunicaciones, telemática y de las interfaces". **(s/a, TICs en el aula)**

Definiendo este apartado **(s/a, Universidad de Los Andes, 2001, pág. 01)** Las Tecnologías de la Información y la Comunicación (TIC) han permitido el desarrollo de sistemas de comunicación mediante computadoras, cuyo exponente paradigmático es la Internet, que ha sido definida como "la red de redes". **(Aguado, 2011, pág. 20)** profundiza: "La Teoría Matemática de la Información, la Teoría de Sistemas y la Cibernética introducen las ideas de comunicación e información en el corazón de la cuestión del método de conocimiento, hasta el punto de que **se considera a la información como la unidad de la que se compone el conocimiento y a la comunicación como el proceso por el cual puede incrementarse el conocimiento**"; **(Aguado, 2011, pág. 21)** "La proximidad entre las ideas de "Sociedad de la Información" y "Sociedad del Conocimiento" en un contexto sociocultural donde las tecnologías y los procesos de comunicación son el referente básico hace patentes las profundas implicaciones del concepto".

B. Aplicaciones de Internet

Se denomina aplicación web dentro de la ingeniería de software a aquella herramienta que permite a los usuarios acceder a Internet.

> Una aplicación informática es un tipo de software que permite al usuario realizar uno o más tipos de trabajo. Son, aquellos programas que permiten la interacción entre usuario y computadora (comunicación), dando opción al usuario a elegir opciones y ejecutar acciones que el programa le ofrece. Existen innumerable cantidad de tipos de aplicaciones. Los procesadores de texto y las hojas de cálculo son ejemplos de aplicaciones informáticas, mientras que los sistemas operativos o los programas de utilidades (que cumplen tareas de mantenimiento) no forman parte de estos programas. Las aplicaciones pueden haber sido desarrolladas a medida (para satisfacer las necesidades específicas de un usuario) o formar parte de un paquete integrado (como el caso de Microsoft Office). A continuación relacionamos algunos ejemplos con quizás las más usuales **(Benítez Jiménez, 2012)**

Las aplicaciones en internet son un conjunto de programas diseñados para la realización de una tarea concreta, como una aplicación comercial, contable, etc. **(s/a, Google)**

Debido a lo fácil que es usar una aplicación de internet hoy en día casi ninguna persona o usuario utiliza Internet sin hacer uso de alguna aplicación "***Actualmente las aplicaciones en internet son de lo más utilizado en la web debido a la gran versatilidad y facilidad de consulta por parte de los usuarios*** cada día se incrementa en la red más grande de todo el mundo que es internet". **(s/a, Google)**

Las aplicaciones online son concretamente programas creados por los desarrolladores que proveen de algunas herramientas a todo usuario que esté conectado a Internet y que acceda a ellas. **(Raiteri, 2011)**

En cuanto a lo que son las aplicaciones de Internet es bueno recordar que esta red cuenta con una estructura, de la cual las aplicaciones son una parte importante, al respecto **(Martin Gavilan, 2009, pág. 3)** detalla "Sobre la estructura de Internet se han desarrollado cuatro grandes tipos de servicios: de comunicación, de conexión, de acceso a la información y móviles. Dentro de estos grandes grupos se encuentras las aplicaciones desarrolladas para los usuarios de esta red.

- Servicios de comunicación: correo electrónico, IRC (chats), listas de distribución, news/USENET (grupos), blogs, wikis y agregadores de contenido (RSS feeds).
- Servicios de conexión: conexión remota (telnet), transferencia de ficheros (ftp), telefonía sobre IP, VPN, Wi-fi, etc.
- Servicios de acceso a la información: portales, buscadores, bibliotecas digitales, etc.

- Servicios móviles: mensajería (SMS), portales, multimedia (MMS), What´s app, etc.

Nuevas características de las aplicaciones de internet

Las redes sociales e Internet de Servicios. Algunas aplicaciones re reciente auge, "tales como los blogs o wikis, la puesta en común de contenidos o la expansión de las redes sociales están ampliando la participación en Internet". Los expertos hablan ya de una ***nueva generación que permitirá la utilización masiva de la red de forma automática***. **(Martin Gavilan, 2009, pág. 13)**

"Internet de los objetos". El concepto de "*Internet de los objetos*" "hace referencia a la conexión sin fisuras de dispositivos, sensores, objetos, espacios, etc., a través de redes fijas o inalámbricas" **(Martin Gavilan, 2009, pág. 15)**.

Uso nómada: Los usuarios se orientan cada vez más hacia dispositivos ligeros tales como los ordenadores portátiles, los asistentes digitales personales (como PDA, Pocket PC o móviles 3G), los reproductores MP3 (iPod), los televisores móviles, los sistemas de GPS o las consolas de videojuegos portátiles. Los usuarios querrán disponer de un acceso fácil y poco costoso a servicios de Internet dondequiera que se encuentren. Esta novedad (una Web 2.0 en movimiento y adaptada a las necesidades del usuario) **(Martin Gavilan, 2009, pág. 15)**.

Retos para la privacidad y la seguridad. La privacidad de la red es ya motivo de preocupación. La Internet del futuro no hará sino aumentar las exigencias de una red más sólida y segura. Se prevén riesgos derivados de la creación de perfiles de usuario, el uso de identificadores de usuarios o de objetos ligados a etiquetas inteligentes por radiofrecuencias (RFID), el tratamiento invisible de información, el cruce de datos y la divulgación de información, así como la reutilización

de información personal procedente de redes sociales **(Martin Gavilan, 2009, pág. 16)**.

Entre los factores de vulnerabilidad de la red está la posible falta de garantías en la protección de datos y seguridad adecuada de la información, y no sólo por parte de la ciberdelincuencia. Actualmente, grandes corporaciones, proveedores de información y de servicios en la red, poseen mucha (demasiada) información sobre nuestro uso de Internet, y a partir del tratamiento de esa valiosa información son capaces de diseñar modelos de negocio y generar nuevas necesidades a los usuarios. Estas prácticas, inadmisible éticamente e inaceptable social y políticamente, deberán ser algún día reguladas. Es claramente necesario tomar medidas para que la Internet del futuro sea segura desde su concepción. **(Martin Gavilan, 2009, pág. 16)**

C. Usuario de Internet

El término ¨usuario de Internet¨ según la **(Universidad de Palermo, pág. 02),** se refiere a "*la* ***persona física o legal que está usando el servicio de acceso a Internet, y en esa capacidad tiene la libertad de impartir y recibir información, y utilizar u ofrecer aplicaciones y servicios a través de dispositivos de su elección****. Cualquier persona legal que ofrezca contenido y/o aplicaciones en Internet también es un usuario de Internet*", de otro lado y complementando la idea señalada, tenemos a **(Wikipedia (B), 2014)** que define el término "usuario informático" donde "*Según la Real Academia Española, un usuario es «aquél que usa algo» o «que usa ordinariamente algo». Por ejemplo un usuario de una biblioteca es un lector interesado en leer algún volumen de su archivo.* ***Sin embargo, esto se opone a los conceptos de la Web semántica, Web 2.0 y 3.0, ya que la realidad actual prima a los ciudadanos como emisores y no solo como receptores que «usan» los medios. Es preferible, por tanto, hablar de actores, sujetos,***

ciudadanos, etc. para referirse a las personas que interactúan en las redes digitales.

Una definición esencial la sostiene el banco mundial "Los usuarios de Internet son personas con acceso a la red mundial" **(s/a, Banco Mundial)**, del mismo modo otra acepción la presenta el diccionario de la Real Academia Española "***un usuario es quien usa ordinariamente algo***. El término, que procede del latín usuarius, hace mención a la persona que utiliza algún tipo de objeto o que es destinataria de un servicio, ya sea privado o público." **(s/a, Definicion.de)**, por último una acepción de usuario de Internet algo más enfocada en la materia que se está tocando es "En informática, ***un usuario es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona.***" **(s/a, Alegsa.com)**

i. La persona como usuario de Internet

Desarrollando el tema tenemos a ***(Wikipedia (B), 2014)*** que define el término "usuario informático" donde "*Según la Real Academia Española, un usuario es «aquél que usa algo» o «que usa ordinariamente algo». Por ejemplo un usuario de una biblioteca es un lector interesado en leer algún volumen de su archivo.* ***Sin embargo, esto se opone a los conceptos de la Web semántica, Web 2.0 y 3.0, ya que la realidad actual prima a los ciudadanos como emisores y no solo como receptores que «usan» los medios. Es preferible, por tanto, hablar de actores, sujetos, ciudadanos, etc. para referirse a las personas que interactúan en las redes digitales***.

Disgregando la idea abordada, tenemos un término que aparece en relación, "los tipos de usuario informático", a lo cual **(Wikipedia (B), 2014)**presenta "En sentido general, **un usuario es un conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso**.

Es decir, un usuario puede ser tanto una persona como una máquina, un programa, etc".

Usuario anónimo

Un usuario anónimo en informática es **aquel que navega en sitios web (o usa cualquier servicio de la Internet) sin identificarse como usuario registrado. En algunos servicios de Internet se dispone de un modo de uso como usuario registrado y otro como usuario anónimo; normalmente, el usuario registrado goza de mayores privilegios**. El anonimato en Internet es uno de sus puntos fuertes, a la vez que motivo habitual de discusión. **A los usuarios les gusta sentirse libres para expresarse, mientras que ciertos organismos quisieran un mayor control de todo el movimiento por la red para actuar con más eficacia contra la delincuencia en línea.** Para contrarrestar el anonimato se pueden llegar a utilizar «alias».

Usuario beta tester

En el proceso del desarrollo de software, existe un usuario intermedio entre el desarrollador y el usuario final, que se encarga de comprobar que el programa trabaje de la forma prevista. La tarea de los beta testers es reportar errores al programador/desarrollador, y es en gran medida responsable de que el programa llegue al usuario final sin errores.

Continuando con la línea de ideas presentadas, un concepto de usuario poco frecuente de utilizar es aquel en el que prima su experiencia, al respecto **(Wikipedia (B), 2014)** nos presenta una definición: "Aunque las personas que tienen contacto directo con las computadoras pueden ser definidas colectivamente como usuarios, de forma individual tienen numerosas diferencias (edad, sexo, conocimientos previos, motivación, etc.). Sin embargo, hay situaciones en que es necesario clasificarlos en una sola categoría; por ejemplo, para fines de evaluación. **Una de las más utilizadas es la que clasifica a los**

usuarios según su nivel de conocimiento (avanzado, principiante, intermedio). Ya Sutcliffe (1988) lo define de la siguiente manera:

Inexpertos: son las personas que no tienen experiencia en el uso de máquinas y tecnología.

Principiantes: personas que han tenido algún contacto con maquinaria y tecnología;

Habilitados: **son usuarios competentes, pero que les falta algo (al nivel de conocimiento o comprensión) que les permitan ser clasificados como expertos**. Se podría decir que la mayoría de los usuarios entran en esta categoría.

Expertos: se trata de individuos que poseen tan vasto conocimiento sobre la maquinaria y tecnología, que serían capaces de desmontarla y volver a montarla si fuera necesario. Constituyen un grupo relativamente pequeño de personas.

> Otra clasificación la presenta wikipedia estableciendo: "Hackos (1994) sugirió que debería haber una categoría de «usuarios en transferencia» para incluir los habilitados que están aprendiendo una nueva aplicación (convirtiéndose temporalmente en «novatos»). Ha recomendado también que se tuviera en cuenta el tipo de uso: los «usuarios por repetición» serían aquellos que pueden utilizar el sistema de manera competente, desde que sigan instrucciones y rutinas. Es decir: aunque podrían ser clasificados como usuarios habilitados, su falta de entendimiento los excluye de este grupo. **En 1998, Hackos y Redish han emitido su propia clasificación, basada en la de Dreyfus y Dreyfus (1986): usuarios principiantes, principiantes avanzados, usuarios competentes y usuarios expertos**. Esta escala de progresión continua permite ordenar a todos los usuarios en alguna de sus etapas, pero no toma en cuenta que alguien puede ser apto en alguna aplicación y novato en otra. En 1982, Carey había sugerido un modelo bidimensional que tuviese en cuenta la capacidad para

las aplicaciones en general y en programas específicos. La clasificación propuesta por ella fue: **inexperientes** (una persona con un conocimiento mínimo, sea de la aplicación, sea del sistema), **principiantes** (poco conocimiento de la aplicación, pero conocimiento sustancial del sistema), **ocasionales** (que tienen un conocimiento considerable de la aplicación, pero conocimiento limitado del sistema) y **expertos** (que tienen un conocimiento considerable de los dos aspectos). En 1997, **Smith añadió una tercera dimensión al modelo, el conocimiento general de tecnología de la información (alfabetización informática)**, lo que le permitió crear el «cubo del nivel de habilidad del usuario». Al clasificar en alto o bajo el conocimiento de la aplicación, del sistema y de la alfabetización informática, Smith ha generado ocho tipos diferentes de usuarios: principiantes, «loros» (que solo repiten lo que se les enseña), alfabetizados, capacitados, ocasionales, específicos, en transferencia y expertos. **Una característica común a todas las clasificaciones de usuarios es que tarde o temprano, todos ellas resultan ser problemáticas. Por lo tanto, como regla general, la clasificación en tres niveles básicos (avanzado, principiante, intermedio), debe ser más que suficiente para establecer el nivel de habilidad de los usuarios**." **(Wikipedia (B), 2014)**

2.2.5 NORMATIVA Y ORGANISMOS NACIONALES

A. Regulación nacional

Ley de protección de datos personales

La ley bajo análisis, se basa en el derecho a la protección de datos. En este sentido, la Ley señala como **facultades el acceso, supresión y oposición, los mismos que pueden ser limitados a fin de proteger derechos e intereses de terceros**, o cuando se puedan ver obstaculizadas actuaciones judiciales o administrativas en curso,

vinculadas al cumplimiento de obligaciones tributarias o previsionales, investigaciones penales, desarrollo de actividades de control de la salud y del medio ambiente, verificación de infracciones administrativas u otros supuestos que establezca la ley.

B. La Dirección General de Protección de Datos Personales

Es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales, su competencia es de aplicación nacional, es un órgano que depende jerárquicamente del Despacho Viceministerial de Derechos Humanos y Acceso a la Justicia. Le corresponde realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la Ley de Protección de Datos Personales – Ley Nº 29733 y su Reglamento.

Se encarga de supervisar la administración y actualización del Registro Nacional de Protección de Datos Personales, así como resolver las reclamaciones formuladas por los titulares de datos personales en tutela de sus derechos de ARCO. Asimismo, emite opinión técnica vinculante respecto de los proyectos de normas que regulen los datos personales y emite las directivas para la adecuada aplicación de la Ley de Protección de Datos Personales y su Reglamento; ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras a través de las siguientes unidades orgánicas:

Dirección de Registro Nacional de Protección de Datos Personales
Dirección de Supervisión y Control
Dirección de Sanciones
Dirección de Normatividad y Asistencia Legal

C. La Oficina Nacional de Gobierno Electrónico e Informática

La (ONGEI), es el Órgano Técnico Especializado que depende directamente del Despacho de la Presidencia del Consejo de Ministros (PCM). ONGEI, en su calidad de ente Rector del Sistema Nacional de

Informática, ***se encarga de liderar los proyectos, la normatividad, y las diversas actividades que en materia de Gobierno Electrónico realiza el Estado.*** Entre sus actividades se encuentran, las vinculadas a la normatividad informática, la seguridad de la información, el desarrollo de proyectos emblemáticos en Tecnologías de la Información y la Comunicación (TIC), brindar asesoría técnica e informática a las entidades públicas, así como, ofrecer capacitación y difusión en temas de Gobierno Electrónico y la modernización y descentralización del Estado. **(ONGEI, 2014)**

La ONGEI, asimismo, ***se encarga de la administración de diversos portales del Estado***, entre los que se encuentran el Portal del Estado Peruano (PEP), el cual es el de mayor jerarquía a nivel de Estado, que se constituye en el sistema interactivo de información a los ciudadanos a través de Internet; el Portal de Servicios al Ciudadano y Empresas (PSCE), el Portal de la Comisión de Comisión de Desarrollo de la Sociedad de la Información (CODESI), entre otros.

El Gobierno Electrónico, según la Organización de las Naciones Unidas (ONU), es el uso de las Tecnologías de la Información y la Comunicación (TIC), por parte del Estado, para brindar servicios e información a los ciudadanos, aumentar la eficacia y eficiencia de la gestión pública, e incrementar sustantivamente la transparencia del sector público y la participación ciudadana **(ONGEI, 2014)**.

2.2.6 ANÁLISIS INTERNACIONAL

A. Análisis Comparado

i. Marco jurídico en la Unión Europea

Respecto al tema, **(Cristos Velasco, 2004, pág. 2)** señala: "Muchos países, como por ejemplo algunos estados miembros de la

Unión Europea han considerado los temas de privacidad y protección de datos personales como asuntos prioritarios en su agenda legislativa, con el propósito de hacer no sólo un frente comercial común a fuertes bloques comerciales regionales como son el TLCAN y el MERCOSUR, sino sobre todo como una medida proteccionista para salvaguardar y proteger los derechos y libertades de las personas físicas, en particular del derecho a la intimidad y la libre circulación de datos personales, derechos consagrados en las constituciones y leyes de los estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, buscando con base en estos ordenamientos jurídicos, proteger a los ciudadanos europeos al momento en que proporcionen información personal a empresas, filiales, sitios y organismos gubernamentales y no gubernamentales en línea que se encuentren físicamente localizados dentro del continente europeo o que tengan sus servidores fuera de países miembros de la Unión Europea.". "La "Directiva 95/46 del Parlamento Europeo y del Consejo del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos"...,...Esta Directiva establece reglas muy estrictas para la protección de los derechos y garantías de libertad de los ciudadanos europeos y en particular la protección del derecho a la privacidad con relación a la obtención y procesamiento de datos personales."

Un aspecto importante a señalar lo refiere **(Cristos Velasco, 2004, pág. 3)** "Una de las disposiciones más controvertidas que contiene esta Directiva es el artículo 25, que establece la prohibición a sus estados miembros de transferir datos personales e información a terceros países que no proporcionen una suficiente y adecuada protección a la privacidad".

A modo de análisis y comentario **(Cristos Velasco, 2004, pág. 4)** resalta: "El artículo 25 de la Directiva sobre Privacidad y Protección de

Datos contiene una clara restricción comercial que ha tenido un grave impacto a nivel mundial, sin embargo, en el caso de países latinoamericanos como Argentina, Chile y Paraguay han introducido legislación sobre protección de datos consistente con esta Directiva, con el objeto de estrechar sus lazos comerciales y diplomáticos con el continente europeo, sin tomar en cuenta que la prohibición del libre flujo transfronterizo de datos e información podría ocasionarles graves distorsiones comerciales con terceros países como los Estados Unidos y Canadá que eventualmente los podrían llevar a tener que sustanciar una controversia en el ámbito de la Organización Mundial del Comercio (OMC)."

ii. Alemania

En el caso de Alemania los primeros intentos de abordar una normativa de protección de datos en función del usuario se dio durante los años 70, es así como nos lo relata **(Saltor, 2013, pág. 202)** "*Alemania cuenta con el antecedente de haber legislado la primera ley europea de las llamadas leyes de primera generación de protección de datos en el Estado de Hesse. Promulgada el 7 de octubre de 1970, esta norma provincial fue precursora en su tiempo y solitaria en su territorio*".

Después de los primeros intentos por legislar el tema bajo análisis, **(Saltor, 2013, pág. 202)** Alemania, tuvo que aguardar casi siete años para formular su primer cuerpo normativo en relación a los datos de la persona y su derecho de personalidad, veamos: "...hasta que se promulgó, el 27 de enero de 1977, la Ley Federal para la protección contra el uso ilícito de Datos Personales. En la actualidad, la ley de protección de datos en Alemania es la conocida BDSG de 20 de diciembre de 1990 que entrando en vigor el 1 de junio de 1991 sustituye a la de enero de 1977 y su objeto es "***Proteger al individuo para que la utilización de los datos personales no comporte un atentado a su derecho a la personalidad***".

Sin embargo para el caso alemán existe toda una suerte de excepciones que permiten utilizar datos personales sin el consentimiento de su titular, veamos: "…sólo se podrá sortear el consentimiento del titular por medio de una ley del Estado o cuando un interés superior esté en juego y en todo caso se establece dentro de las disposiciones generales el secreto profesional que garantice, aun con el tratamiento de los datos, unos niveles mínimos de confidencialidad" **(Saltor, 2013, pág. 203)**.

Tal como se dijo el estado puede crear normas que exceptúen el consentimiento del titular en la tratativa de datos personales, para ello tenemos como ejemplo: "*Las oficinas públicas pueden recolectar y reproducir información, solo en cumplimiento de sus misiones específicas. La creación de un registro público debe ser comunicada al ciudadano y publicada en el Boletín Oficial, con excepción de las cuestiones relacionadas con el servicio de información federal, con el servicio de seguridad militar, con la defensa de la Constitución Federal y la defensa nacional*" **(Saltor, 2013, pág. 203)**.

"*El sistema de protección de los datos personales de la ley alemana no es de aplicación a las personas jurídicas, quedando una referencia expresa a su aplicación solamente a las personas físicas al definir los datos objeto de protección como los concernientes a las informaciones individuales sobre la situación personal o material de una persona física determinada o determinable*" **(Saltor, 2013, pág. 203)**.

"La ley se aplica a todo tipo de registro, sean automáticos o manuales, públicos o privados, siempre que en ellos se procesen datos personales. El objeto de la ley se extiende también a los archivos manuales cuando los datos se encuentren bajo una estructura lógica que permita que sean objeto de tratamiento automatizado. La ley textualmente dice: Toda colección de datos estructurados de la misma forma y

susceptibles de ser clasificados, tratados y explotados según unos criterios definidos. Los archivos o registros de datos necesitan autorización legal para su habilitación" **(Saltor, 2013, pág. 203)**.

"El Registro de Bancos de Datos Automáticos está a cargo de un funcionario calificado como Delegado Federal para la Protección de Datos Personales, el cual es designado por el Presidente de la República. El sistema distingue los Bancos de Datos denominados propios, que no poseen regulación de ningún tipo, con mínima intervención de la autoridad" **(Saltor, 2013, pág. 203)**.

En este fallo el TC (Tribunal constitucional) alemán sentó las bases de la doctrina de la autodeterminación informativa.

(Klink, 2011, pág. 88) Señala en su artículo "**La actual posición del Tribunal Supremo alemán ante la libertad de expresión en la red, el caso de la "chuleta" – "spickmich.de"**", La sentencia del 23 de junio de 2009 es la primera sentencia del Tribunal Supremo alemán sobre los portales de evaluación en Internet que afectan al derecho de la personalidad. *Según esta sentencia clave, los portales de evaluación en Alemania son admisibles si se respetan los criterios mencionados en la sentencia. La sentencia del Tribunal Supremo da pautas importantes para el tratamiento jurídico de evaluaciones en Internet. No obstante,* ***la admisibilidad siempre depende de una ponderación entre el derecho de la personalidad y de la libertad de comunicación***. En el caso decidido, la libertad de comunicación prevaleció sobre el derecho de la personalidad de una profesora de colegio evaluada en el portal spickmich.de. Considerando las restricciones del acceso, el pequeño valor informativo de las evaluaciones, la escasa intervención en los derechos de la profesora y el interés legítimo a la información, el Tribunal Supremo ha desestimado la demanda de la profesora.

iii. España

España como país europeo, gracias a las novísimas corrientes que protegían los datos personales de las personas allá por los años 70, lo estableció en su constitución de 1978, veamos:

> "...los constituyentes españoles de 1978 pensaron que el desarrollo de las nuevas tecnologías de la información y las telecomunicaciones era una amenaza para los derechos fundamentales de los ciudadanos. Para evitar el peligro que les representaba el desarrollo tecnológico de las TIC, incorporaron en la Constitución española, en el artículo 18.4, una garantía de protección a las personas frente a la informática. Esta norma, presente en la Constitución, tiene por objeto limitar el uso de la informática para garantizar el honor, la intimidad familiar y personal de los ciudadanos junto al pleno ejercicio de sus derechos". **(Saltor, 2013, pág. 192)**

Los constituyentes españoles tuvieron a la vista el artículo 35 de la Constitución Portuguesa de 1976 junto a las diferentes leyes ya existentes en algunos Estados europeos, ***de protección de datos y defensa de la intimidad frente a la informática***, por ejemplo las danesas y alemanas, que incidieron en la actitud de los parlamentarios españoles desde los primeros debates sobre la nueva Constitución **(Saltor, 2013, pág. 192)**.

Antes de ocuparnos de la LOPD[15], es necesario un comentario sobre la ley derogada, dado que sus efectos se sintieron tanto dentro como fuera de España y su articulado sirvió de fuente para leyes de otros estados, en particular de Latinoamérica. A modo de ejemplo podemos mencionar la vigente ley argentina Nº 25.326 de Protección de Datos Personales promulgada en el año 2000, en la cual se observa una fuerte influencia de la LORTAD **(Saltor, 2013, pág. 192)**.

La LORTAD fue la primera ley orgánica española referida a la protección de los datos de carácter personal que vino a cumplir con el expreso mandato constitucional del artículo 18.4, que ordenaba al

[15] *Ley Orgánica de Protección de Datos*

legislador español que dictara una norma de tutela de las libertades en relación con el uso de la informática, y con diversos acuerdos internacionales que contaron con la adhesión española **(Saltor, 2013, pág. 192)**.

> *Para ello, este acuerdo regula el flujo de informaciones personales en función de la cooperación policial.* ***El Sistema de Información de Schengen (SIS) tiene como objetivo principal la comunicación de informaciones para el control de las personas "indeseables" y/o "inadmisibles" dentro del espacio Schengen*** *con una gran base de datos policiales situada en Estrasburgo y sometida a la legislación francesa de protección de datos personales. Para evitar los efectos nocivos del intercambio de información policial, el convenio de Schengen también exigió que cada país signatario incorporara normas internas sobre protección de datos personales que satisfagan los principios del Convenio del Consejo de Europa para la protección de datos personales.* **(Saltor, 2013, pág. 192)**

Respondiendo a estos compromisos internacionales, la LORTAD buscó garantizar en España los derechos y libertades de las personas físicas y en particular su intimidad frente a la utilización de la informática y además cumplir con el mandato constitucional del artículo 18.4 **(Saltor, 2013, pág. 192)**.

> *En el diseño normativo de la LORTAD, el legislador reunió características de leyes de protección de datos de diferentes generaciones: exige una autorización previa a los bancos de datos (aporte de las leyes de primera generación), da una protección especial a los datos sensibles por su inmediata incidencia en la privacidad o de su riesgo para las prácticas discriminatorias (leyes de segunda generación), y limita la cesión de datos, controlando la*

dinámica de su uso y funcionalidad (aporte propio de las leyes de tercera generación). Siguiendo la línea de las leyes de protección de datos de tercera generación, la exposición de motivos de la LORTAD anunciaba la protección de los bancos de datos personales desde una perspectiva funcional que no se limitó a su tutela en cuanto meros depósitos de informaciones, sino como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar un perfil informático personal **(Saltor, 2013, pág. 192)**.

En España, el perfil informático de la persona es considerado, como la reputación o fama, que es expresión del honor y que puede ser valorado favorable o desfavorablemente para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión de determinados colectivos **(Saltor, 2013, pág. 192)**.

iv. Estados Unidos

En línea sucesiva con lo tratado, corresponde analizar la legislación norte americana, cuyas características y puntos de vista la hacen muy particular y sienta referentes para otras legislaciones, veamos: **(Cristos Velasco, 2004, pág. 4)**, "*...ha adoptado una política de autorregulación que ha estado a cargo en gran medida del sector privado, respondiendo satisfactoriamente a las demandas y necesidades de sus grandes corporaciones y protegiendo en la medida de lo posible los derechos básicos de los consumidores y de los ciudadanos con base en la primera enmienda de su Constitución*"

En concordancia con lo analizado y explicado en el parágrafo anterior, se puede deducir que esta normativa presenta muchos sesgos contextuales que hacen posible su aplicación en el "País de las

oportunidades", dado que a su población poco le importa su intimidad en la red, debido a hechos contextuales que definieron a esta población, tal como fue el atentado del 11 de setiembre, esto tiene por consecuencia la sobre flexibilización que tiene la privacidad y la protección de los datos personales, dentro y en concordancia con su esquema liberal, brindando una autonomía regulatoria al sector privado, por el hecho de subvalorar las garantías fundamentales de sus ciudadanos en función al aspecto económico, comercial y de seguridad nacional que adopta este país, sin embargo, es de gran interés resaltar la protección de la información de los niños menores de 12 años, acción orientada fundamentalmente hacia aquellos sitios web frecuentemente visitados por niños.

v. Canadá

Este país por su parte ha adoptado una política de regulación auténtica y mucho más ecléctica que a opinión de **(Cristos Velasco, 2004, pág. 5)**, "...han seguido políticas de regulación sobre privacidad y protección de datos caracterizadas por la adopción de la llamada "Tercera Vía" (The Third Way), es decir, han tratado de adoptar un marco regulatorio que no sea ni excesivamente sobre regulado por el gobierno ni tampoco que sea libremente autorregulado por las empresas, sino que combine legislación y políticas de autorregulación eficientes que respondan específicamente a las necesidades individuales de sus nacionales, **buscando con ello proteger los derechos de los ciudadanos y consumidores, sin menoscabar los intereses patrimoniales de las medianas y grandes empresas**, estableciendo reglas claras y organismos gubernamentales ad-hoc eficientes para su debida vigilancia."

vi. México

El país mexicano, cuenta con una normativa que explicada en palabras de **(Cristos Velasco, 2004, pág. 9)**, detalla: "El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos representa el

marco jurídico de la privacidad en nuestro país. El primer párrafo de este artículo consagra una de las garantías individuales más importantes que es el derecho que tenemos a no ser molestados en nuestra persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.", además cuenta con adelantos jurídicos muy acertados en relación a la protección de datos personales, **(Cristos Velasco, 2004, pág. 9)** "...la protección de datos personales en el área ... ya se encuentra regulada en la Ley Federal de Protección al Consumidor (LFPC) y actualmente dicha legislación contempla la posibilidad de que los proveedores y consumidores puedan celebrar transacciones a través de medios electrónicos. La fracción I del artículo 76 bis de la LFPC le impone la obligación a los proveedores de mantener la confidencialidad de la información y la prohibición de difundirla o transmitirla a otros proveedores, a menos que el consumidor lo haya autorizado por escrito..."

vii. Brasil

"*Sin derecho a la privacidad no se tiene una real libertad de expresión y de opinión, entonces no hay democracia. Estamos ante una grave violación de los derechos humanos y las libertades civiles*"

"*El ciberespacio no puede ser utilizado o manipulado como arma de guerra a través del espionaje*"

Dilma Rousseff

Sin duda alguna el año 2014 será considerado el año en que Brasil sentó precedentes sobre la regulación normativa de Internet, no solo por proponer la norma más avanzada en materia de protección y gobernanza de Internet para su momento, sino por garantizar derechos y obligaciones en la red, tanto para usuarios, como para proveedores de conexiones y de aplicaciones, este apartado convierte a esta norma en pionera de grandes avances en la materia, garantizando un equilibrio entre derechos y

conservando la esencia de la red, es decir, abierta y descentralizada, este marco fue promulgado bajo el impulso de la presidenta brasileña Dilma Rousseff a un día del evento NetMundial que se realizó del 22 al 24 de abril en Sao Paulo, frente a representantes de 85 países, asimismo, en dicho evento asistieron referentes de diferentes disciplinas, trayectorias y partes del planeta.

La norma en mención comenzó a constituirse en el año 2009, contando con la participación de diferentes entidades en su diseño **(Poire, 2014)** "El proyecto fue construido a partir de la participación ciudadana, de diferentes sectores políticos, movimientos sociales y organizaciones que expusieron sus puntos de vista y preocupaciones sobre cómo regular la red. A través de espacios online y offline se articularon debates y aportes, se hicieron enmiendas y aclararon aspectos determinantes".

> "El marco civil brasileño fue saludado como un ejemplo para el mundo, un instrumento importantísimo para mejorar y democratizar la gobernanza global de internet, para construir consensos y tornarla cada vez más abierta, multisectorial, multilateral, democrática y transparente. Estos son objetivos con que el mundo tiene que preocuparse inmediatamente frente a los inaceptables y condenables episodios de monitoreo y espionaje en la red" Dilma Rousseff en Café con la Presidenta **(Poire, 2014)**

La mencionada norma contó con diversos sectores de apoyo, entre ellos importantes personalidades que se consideran referentes en la red, como por ejemplo a Tim Berners Lee, creador de la web, entre otros.

La creación y aprobación del marco civil brasileño no fue fácil, así como veremos más adelante:

> "Dijo Marcelo Branco, en una interesante entrevista a la Agencia Paco Urondo. Branco es militante de la libertad del

conocimiento y software libre, quien trabajó junto a Lula desde el principio y hoy es encargado de la comunicación en redes sociales de Dilma Rousseff, Adjudicó la demora en la sanción de la ley se debió por un lado al lobby contra la neutralidad de la red ejercido por los monopolios de telecomunicaciones y, por otro, al esgrimido por las industrias culturales defensoras del copyright, a las que llamó las "mafias del copyright" que pretendían poder sacar de circulación contenido sin previa orden judicial". **(Poire, 2014)**

¿Qué implica el Marco Civil?

El Marco civil brasileño contempla ***derechos y obligaciones de los ciudadanos y los proveedores*** (tanto de conexión como de aplicaciones) ***en relación a la protección de datos personales*** (esos que empresas compran y venden sin nuestra autorización), a la neutralidad de la red en el sentido que no pueda cobrarse de manera diferenciada según navegación (como pasa con el cable que ofrece diferentes paquetes de contenidos y canales) y ***que se garantice acceso y calidad de servicio,*** al mismo tiempo que aboga por el respeto de la libertad de expresión en el sentido que ***no puede eliminarse contenido sin la orden de un juez y que el responsable por lo publicado es el usuario*** (no el proveedor de conexión o aplicación) **(Poire, 2014)**.

En conjunción a lo expresado:

"**Lleva al ambiente virtual la misma regla que vale para cualquier espacio público**. Las personas son responsables por lo que dicen. Con eso, trae un equilibrio entre las garantías constitucionales de protección de la libertad de expresión y de protección de la intimidad, de la honra e imagen de las personas. Además, la regla es clara: los derechos offline tendrán que ser los

mismos derechos garantizados al ciudadano online." Dilma Rousseff en Café con la presidenta. **(Poire, 2014)**

Contempla la creación de juzgados especiales a los que los ciudadanos pueden reclamar en casos que sientan que sus derechos no han sido respetados. Especialmente será útil en casos en que personas violen la privacidad e intimidad de otras, o se sientan agraviados o amenazados por los contenidos publicados por otros. Sólo en esos casos y mediante la resolución de estos juzgados se podrá dictaminar que el contenido debe ser retirado.

La norma establece que empresas multinacionales como Facebook y Google se sometan a los fallos de las cortes nacionales que involucren a usuarios brasileños. También busca fortalecer la neutralidad de la red, al impedir que las compañías prestadoras de servicios cobren tarifas diferenciadas en función del consumo de ancho de banda **(Marty, 2014)**.

En síntesis estos son los principios en los que se basa:

- Garantizar la libertad de expresión
- Protección de la privacidad de los datos personales
- Neutralidad de la red
- Libertad de los modelos de negocios

Los derechos que garantiza:

- Control sobre los datos personales
- Inviolabilidad y secreto de las comunicaciones
- Mantenimiento de la calidad contratada de la conexión.
- Exclusión definitiva de los datos personales una vez terminados los contratos

Información clara y completa en los contratos.

Las obligaciones que estipula para los proveedores

De conexión: guardar bajo secreto los datos de conexión de los usuarios (dirección IP, fecha, hora y tiempo de conexión) por 1 año

De aplicaciones: guardar datos de navegación de los usuarios por seis meses.

Los proveedores, también los extranjeros (Facebook, Google, Twitter...), deberán respetar las leyes brasileñas incluyendo las de derecho a la privacidad y secreto de los datos. Este punto es fundamental puesto que la mayoría de los proveedores de aplicaciones tienen sus sedes y bases de datos en otros países lo que constituye un obstáculo central cuando una persona pretende denunciar un contenido o usuario.

"La neutralidad impide que provedores de conexión provilegien el acceso a determinados sites y servicios en razón de acuerdos económicos (...) Todo el mundo debe poder intercambiar información, conocimiento con todo el mundo en internet, sin bloque, sin interferencia, sin censura.La gran ventaja de internet es permitir que cualquier persona con mucho o poco dinero, pueda divulgar sus ideas, sus servicios o su empresa" Dilma Rousseff en Café con la Presidenta

El Marco Civil de Brasil será necesariamente el punto de partida para cualquier discusión. Es cierto que cualquier ley es perfectible, también hay que reconocer que hay voces en contra, pero lo que es innegable es que constituye un avance importantísimo en materia de derechos.

Dentro de las críticas a la normativa brasileña, Daniel Marchi explica:

> "Internet es el ejemplo más claro de cómo funcionan los mercados libres. Afirma que si bien la red no es perfecta, "la competencia y el sistema de precios pueden garantizar los derechos de los usuarios mucho más efectivamente que la regulación". En su opinión, la verdadera motivación de la regulación

de Internet es que "a los gobiernos no les gusta la libre circulación de información. Venezuela ha sido un excelente ejemplo de eso. Turquía también. Sin hablar de Cuba, Irán o China, donde Internet ha sido censurado sistemáticamente."" **(Marty, 2014)**

Sin embargo la opinión vertida, no aporta soluciones a la protección de los derechos fundamentales de los usuarios, en los aspectos que tienen que ver con la Intimidad y privacidad principalmente.

B. OCDE: Directrices sobre la protección de la intimidad y los datos personales

Desarrollando y analizando tendidamente a este organismo internacional, **(Cristos Velasco, 2004, pág. 7)** menciona: "Las guías de la OCDE que regulan la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales del 23 de septiembre de 1980 contienen ocho principios complementarios de aplicación nacional y cuatro de aplicación internacional que son considerados como los estándares mínimos a seguir para la obtención, el procesamiento de datos y el libre flujo transfronterizo de datos para los sectores público y privado."

El desarrollo del tratamiento automático de datos, que permite ***la transmisión de enormes cantidades de ellos en segundos a través de las fronteras nacionales y, naturalmente, a través de los continentes, ha hecho que sea necesario considerar la protección de la intimidad en relación a los datos personales.*** Se ha introducido, o se van a introducir en breve, legislación para la protección de la intimidad en aproximadamente la mitad de los países miembro de la OCDE (Austria, Canadá, Dinamarca, Francia, Alemania, Luxemburgo, Noruega, Suecia y los Estados Unidos han aprobado legislación; Bélgica, Islandia, Países Bajos, España y Suiza han elaborado proyectos de ley) para impedir lo que se considera que son vulneraciones de derechos humanos

fundamentales, tales como el almacenamiento ilícito de datos personales, exactos o inexactos, o el abuso o la revelación no autorizada de los mismos.

Por otra parte, existe el peligro de que las disparidades en las legislaciones nacionales pudieran obstaculizar la libre circulación transfronteriza de datos personales; circulación que se ha incrementado en gran medida en años recientes y que van a aumentarse aún más con la introducción generalizada de nuevas tecnologías de informática y de comunicaciones. Las restricciones a esta circulación podrían ocasionar graves trastornos en importantes sectores de la economía, tales como la banca y los seguros.

Por este motivo, los países miembro de la OCDE han considerado necesario ***elaborar Directrices que ayuden a armonizar la legislación nacional relativa a la intimidad y que, a la vez que defiendan tales derechos, impidan interrupciones en la circulación internacional de datos***. Representan un consenso sobre principios básicos que pueden incorporarse a la legislación nacional existente o servir de fundamento para la legislación en aquellos países que todavía no dispongan de ella.

Nuestra legislación en cuanto a la protección de datos y la protección de nuestra autodeterminación informativa, ha implementado una serie de principios que entran en directa concordancia con los establecidos por la OCDE, a continuación se desarrollan de forma ampliada:

i. Principios básicos

Principio de limitación de la recogida

Marca los límites en la recogida de datos personales y tales datos deben recabarse mediante medios lícitos y justos y, en su caso, ***con el conocimiento o consentimiento del sujeto de los datos***.

Principio de calidad de los datos

Los datos personales ***deben ser pertinentes para los efectos en los que se vayan a utilizar y, en la medida necesaria a tales efectos***, deberían ser exactos y completos, y mantenerse al día.

Principio de especificación de la finalidad

Cuando se recojan los datos personales ***se debe especificar en el momento de la recogida cuál es su finalidad***, a más tardar, y la posterior utilización quedar limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que se cambie la finalidad.

Principio de limitación de uso

Los datos personales no deberían revelarse, es decir deben mantenerse en estricta confidencialidad, hacerse disponibles o utilizarse de otro modo a efectos que no sean los especificados, salvo:

a) con el consentimiento del titular de los datos, o

b) por imperativo legal.

Principio de salvaguardas de seguridad

Los datos personales deben protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados.

Principio de apertura

Relacionado con una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberían existir medios fácilmente disponibles para establecer la existencia e índole de los datos personales, ***y de las principales***

finalidades para su uso, así como la identidad y domicilio del controlador de los datos.

Principio de participación individual

La persona debería tener derecho a:

a) recabar, del controlador de los datos o de otro modo, confirmación de si el controlador tiene o no tiene datos correspondientes a la misma;

b) hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible;

c) impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos.

Principio de responsabilidad

El controlador de datos ***debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos***.

De dichos principios conviene retroalimentar solo dos, en razón a la esencial relación que guarda para con el presente trabajo, a los que, en el más juicioso detalle se va a abordar y analizar convenientemente relacionándolos de acuerdo a nuestra realidad.

"El principio de "*especificación de la finalidad*", consistente en ***especificar el propósito de recabar información en el momento en el que se lleva a cabo la recolección y el subsecuente uso limitado*** del cumplimiento de dichos propósitos u otros que no sean incompatibles con aquellos propósitos especificados en cada ocasión"

Implicaría que al momento de aceptar las condiciones y términos de servicio, esta sea congruente y válida respecto a nuestra legislación, por ello no debe cederse dicha información si es solicitada por algún organismo, gobierno o entidad que la solicite sin nuestro consentimiento o notificación oportuna.

En segundo lugar "El principio de "*salvaguardas de seguridad*", ***consistente en proteger los datos personales e información, mediante mecanismos razonables de seguridad en contra de riesgos tales como pérdida, acceso no autorizado, destrucción, utilización, modificación o divulgación de datos***"

Pero, qué hacer si realizan actos jurídicos contrarios y por medios que no hemos autorizado o tenemos conocimiento, para empezar como lo sabemos si no hay alguna entidad que controle las extralimitaciones señaladas, a los que nosotros como personas, nos vemos imposibilitados de reclamar o pedir se nos restituya un derecho, no se puede cancelar alguna información o pedir su modificación, al cual somos negados sin nuestro consentimiento, un ejemplo de ello sería, pedir que se nos restituya alguna cuenta en Internet negando el hecho de que hemos violado las condiciones y términos de servicio de nuestra parte (qué entidad nos permite hacer una trámite al respecto) y sin embargo existe una ley que permite las notificaciones electrónicas sin considerar el secuestro o pérdida de las mismas.

2.3 BASES LEGALES

2.3.1 1997 – Ley 26775 – Ley que regula el Derecho de rectificación de personas afectadas por afirmaciones inexactas en medios de comunicación social

2.3.2 2001 – Ley 27489 – Ley que regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información. "Tiene por objeto regular el suministro de información de riesgos en el mercado, garantizando el respeto a los derechos de los titulares de la misma, reconocidos por la Constitución Política del Perú y la legislación vigente, promoviendo la veracidad, confidencialidad y uso apropiado de dicha información".

2.3.3 2002 – Ley 27863 – Ley que Modifica varios artículos de la Ley que regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información

2.3.4 2002 – Ley 27697 – Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional

2.3.5 2007 – DL 991 – Decreto Legislativo que modifica la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional

2.3.6 2009 – Directiva 005-2009/COD-INDECOPI – Directiva de Operación y Funcionamiento del Registro de Números Telefónicos y Direcciones de Correo Electrónico excluidos de ser destinatarios de Publicidad Masiva – Registro "Gracias... No Insista"

2.3.7 2011 – Ley 29733 – Ley de Protección de Datos Personales.

2.3.8 2012 – Ley 29904 – Ley de Promoción de la Banda ancha y Construcción de la Red Dorsal de Fibra Óptica

2.3.9 2013 – Ley 30096 – Ley de Delitos Informáticos.

2.3.10 2013 – DS 014-2013-MTC Reglamento de la ley 29904

2.4 DEFINICIÓN DE TÉRMINOS BÁSICOS

2.4.1 Derecho fundamental

Para conceptuar debidamente este término, resulta conveniente resaltar la base de los derechos fundamentales y son los derechos humanos, para lo cual **(Derecho.com (A), 2014)** realiza las definiciones terminológicas pertinentes; "Los Derechos Humanos **son los derechos de la persona física que deben ser reconocidos y protegidos por los Estados. Son aplicables en todo tiempo y lugar**. Existen mecanismos de supervisión internacional universales como el Comité del Pacto de Derechos Civiles y Políticos en el seno de la Organización de las Naciones Unidas, o mecanismos regionales, como la Comisión Interamericana de Derechos Humanos. Los Derechos Humanos son propios de la condición humana.

En definitiva, los Derechos Humanos son, principalmente:

- Innatos.
- Universales.
- Exigibles
- Inviolables.
- Innegociables.
- Absolutos.
- Irrenunciables.

Continuando con la línea de ideas, una acepción más precisa en torno al tema que se está explicando, es desarrollada por **(Derecho.com (B), 2014)**, "Los derechos fundamentales **son derechos humanos positivizados en un ordenamiento jurídico concreto**. **Es decir, son los derechos humanos concretados espacial y temporalmente en un Estado concreto**. *Son derechos ligados a la dignidad de la persona dentro del Estado y de la sociedad.* Cabe destacar que a **los derechos fundamentales no los crea el poder político, se impone al Estado la obligación de respetarlos**.

Continuando con la explicación, **(Derecho.com (B), 2014)** refiere: "El derecho fundamental jurídicamente tiene la estructura normativa basada en la capacidad que le permite a la persona efectuar determinados actos, es decir, que **los derechos fundamentales son instituciones jurídicas que tienen la forma del derecho subjetivo. Y la estructura del derecho subjetivo tiene tres elementos: titular del derecho subjetivo, el contenido del derecho subjetivo en el que vamos a distinguir las facultades, por otra parte el objeto del derecho, y un tercer elemento es el destinatario o sujeto pasivo, aquel que está obligado a hacer o no hacer**.

A nivel de legislación comparada, tenemos **(Derecho.com (B), 2014)** "En España, los derechos fundamentales vienen regulados en los artículos 15 a 29 de la Constitución Española.

Derecho a la vida.

Derecho a la libertad religiosa e ideológica.

Derecho a la libertad y seguridad.

Derecho al honor, a la intimidad y a la propia imagen.

...etc.

Otra acepción ampliamente aceptada por doctrinarios y juristas respecto al tema que se está tratando son los derechos constitucionales, a los cual **(Wikipedia (B), 2015)** "**son aquellos incluidos en la norma constitutiva y organizativa de un estado generalmente denominada constitución que se consideran como esenciales en el sistema político y que están especialmente vinculados a la dignidad humana**. Es decir, son aquellos derechos que disfrutan de un estatus especial en cuanto a garantías (de tutela y reforma) dentro del ordenamiento jurídico. Es conocido el planteamiento filosófico-antropológico según el cual donde nace una necesidad surge un derecho; este planteamiento tan lógico aparece por primera vez en "La República" de Platón. **Los derechos constitucionales se clasifican en derechos fundamentales o de**

primera generación, derechos económicos, sociales y culturales o de segunda generación y derechos a un medio ambiente sano o de tercera generación.

Para el análisis de los problemas relativos a los derechos fundamentales, a la vista de la jurisprudencia española y de la doctrina y jurisprudencia alemanas, Brage Camazano propone un método que "distingue entre el ámbito normativo del derecho fundamental, como contenido **ab initio**[16] del derecho fundamental, antes de toda posible restricción; la intervención en el derecho fundamental, que se refiere a las distintas formas de interferencia o injerencia en ese ámbito inicialmente protegido por el derecho; y la justificación constitucional de esa intervención. Es un método de enjuiciamiento que, en buena medida responde a la naturaleza de las cosas, al esquema regla (libertad o derecho) excepción (restricciones de la libertad o derecho) que rige en tantos aspectos o ámbitos del derecho, pero que, a nuestro modo de ver, es antes que nada un expediente técnico que facilita el examen de las cuestiones relativas a los derechos fundamentales y hace más transparente dicho análisis". **(Wikipedia (B), 2015)**

2.4.2 Derecho a la Intimidad

El derecho a la intimidad consiste **(Wikipedia, 2015)** en **la defensa de la persona en su totalidad a través de un muro que prohíbe publicar o dar a conocer datos sobre temas como la religión, la política o la vida íntima**. La revelación de estos datos conlleva a una pena, en algunos países perpetua y en España de 6 o 7 años. El ser humano tiene derecho absoluto a mantener su vida privada y bajo ningún concepto esto puede ser revelado ni siquiera a una persona muy cercana. En ese marco, debe entenderse que **el derecho a la inviolabilidad de correspondencia no se reduce únicamente al ámbito de la correspondencia escrita (es decir, la carta postal), sino que también**

[16] *Locución latina y castellana. Desde el comienzo o desde tiempo inmemorial o muy remoto.*

se extiende a cualquier medio o sistema de comunicación privada de las personas, dado que con el desarrollo y avance de la tecnología, actualmente se cuenta con múltiples formas y sistemas de comunicación privada como son la telefonía fija, telefonía móvil y el correo electrónico. La intimidad es la parte de la vida de una persona que no ha de ser observada desde el exterior, y afecta sólo a la propia persona. Se incluye dentro del "ámbito privado" de un individuo cualquier información que se refiera a sus datos personales, relaciones, salud, correo, comunicaciones electrónicas privadas, etc. **El derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida privada, es decir, de sus sentimientos y comportamientos. Una persona tiene el derecho a controlar cuándo y quién accede a diferentes aspectos de su vida particular**.

La Real Academia presenta una base a la definición que pretende establecer "**intimidad se define como «zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia».**"

2.4.3 Derecho a la privacidad

La privacidad es el interés que los individuos tienen en sostener un espacio personal, libre de interferencias con otras personas y organizaciones.

Otra conceptualización la propone, **(Wikipedia, 2015)** "**la privacidad puede ser definida como aquel ámbito de la vida personal de un individuo, que (según su voluntad) se desarrolla en un espacio reservado y debe mantenerse con carácter confidencial**. Por otro lado, y según el Diccionario de la lengua española de la Real Academia Española, la «privacidad» se define como el **«ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión»**

En este sentido, el artículo 12 de la Declaración Universal de los Derechos Humanos, adoptada por la Asamblea General de las Naciones Unidas, establece que el derecho a la vida privada es un derecho humano, y que:

Nadie será objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Asimismo, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas, consagra, al respecto, lo siguiente:

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación; 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

En el ámbito regional, el artículo 11 de la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica, establece una norma de protección de la honra y dignidad, al señalar:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

2.4.4 Derecho a la protección de datos personales

(Piñar Mañas, 2005, pág. 3) Señala: "El derecho fundamental a la protección de datos personales deriva directamente de la Constitución y atribuye a los ciudadanos un poder de disposición sobre sus datos, de modo que, en base a su consentimiento, puedan disponer de los mismos".

De lo anterior expone **(Piñar Mañas, 2005, pág. 8)**, "**El derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos.**"

CAPÍTULO III

HIPOTESIS Y VARIABLES

3.1 HIPÓTESIS GENERAL

Es probable que la regulación de las aplicaciones de Internet a través de un marco normativo específico, garantice el derecho a la intimidad de los usuarios de internet.

3.2VARIABLES

Variable independiente:

Aplicaciones de Internet

Variable dependiente:

Derecho a la intimidad.

3.2.1 Operacionalización de las Variables

Variable	Dimensión	Indicador	Sub-indicador
V I			
Aplicaciones de Internet	Usuario de Internet	Vulneración	- Análisis de información íntima - Registro de comunicaciones - Limitaciones al derecho de defensa - Cambio de las políticas de privacidad - Por Espionaje
V D			
Derecho a la intimidad	Autodeterminación informativa	Manejo de información	- Destino desconocido de la información - Uso de información íntima - Control desigual de información - Beneficio económico con datos íntimos - Perfiles de navegación online - Tráfico de datos

		Formas de protección	- Registros obligatorios - Cuentas de Internet - Respeto a la normativa nacional - Consentimiento expreso - Derecho al olvido - Derecho de cancelación - Notificar y retirar información - Reparación de daños causados - Avisos de intromisiones

CAPÍTULO IV

METODOLOGÍA DE LA INVESTIGACIÓN

4.1 DISEÑO DE LA INVESTIGACIÓN

El diseño de investigación que se desarrollará es de corte analítico – explicativo, porque está basado en analizar y explicar las injerencias al derecho a la intimidad que suceden cotidianamente. Para ello se pondrá de manifiesto el empleo del ***análisis e interpretación documental,*** pues la presente, es una investigación que en un primer momento, analizará la legislación referente a la Intimidad en los aspectos de privacidad y protección de datos personales, con lo referido a las políticas de privacidad planteadas en las aplicaciones más representativas de Internet, cuyo fin es analizar si los usuarios de las mencionadas aplicaciones, se encuentran protegidos o desprotegidos en sus derechos; de otro lado y como segunda etapa, se puntualizará ***explicativamente*** a través del contraste de la teoría con la realidad las causas por las que los usuarios de Internet, deben ser protegidos por la legislación nacional en un marco normativo específico a los derechos de Internet, garante y protector del derecho a la intimidad de los usuarios de Internet.

4.2 TIPO Y NIVEL DE INVESTIGACIÓN

El presente trabajo de investigación, se encuentra enmarcado dentro del tipo de investigación no experimental, así mismo, según la fuente de información, es de tipo documental; según el nivel de medición y análisis de la información estaría enmarcada como Investigación cualicuantativa.

Por su amplitud: El presente trabajo investigativo es holista, es decir exhaustivo, sistémico o panorámico, porque busca realizar un estudio crítico, detenido, riguroso y profundo, pues comprenderá el derecho constitucional a la intimidad desde múltiples facetas, todas relacionadas al ámbito digital o virtual.

Alcance temporal: La presente investigación, por el tenor de su contenido es de carácter reciente, debido a que el tema de investigación constituye una realidad social de permanente actualidad.

En relación con la práctica: La investigación esta enquistada transversalmente en el derecho, se ubica principalmente dentro del derecho informático y constitucional con algunos atisbos del derecho internacional privado, civil y penal. Es de conocimiento y reflejo de la práctica que nuestro sistema jurídico se encuentra en permanente cambio mejora y actualización, es así que se habla del tránsito o cambio que nuestras instituciones jurídicas están volcando en pro de la modernidad, trasladando lo físico al soporte virtual, dentro de lo cual la intimidad juega un rol importante no solo de cuestión teórica, sino en las repercusiones que trae consigo en la realidad dual, es decir, lo físico y lo virtual.

Por su naturaleza: Este trabajo investigativo, se caracteriza por su naturaleza teórica, pues en el presente estudio confluyen diversos constructos teóricos, que serán contrastados con la realidad, lo cual probablemente tendrá positivos atisbos al tema que se aborda con esta investigación.

Por su carácter: Esta investigación buscará sustentar o explicar las causas o efectos, de la relación del usuario de Internet con las aplicaciones de internet, porque indagará los efectos que para este caso, son las formas de vulneración a la intimidad en Internet.

4.3 ENFOQUE DE LA INVESTIGACIÓN

El enfoque elegido para el presente trabajo investigativo es cualicuantitativa en función a dos razones:

Por un lado es cuantitativa, porque se utilizara la recolección de datos para probar la hipótesis en base a la medición numérica y el análisis estadístico para establecer patrones.

Del otro lado es cualitativa, porque se utilizara el análisis documental, para sustentar conceptualmente diversas teorías, concertando la teoría con la realidad, a través de la interpretación de datos y el correspondiente método de análisis hermenéutico.

4.4 MÉTODO DE INVESTIGACIÓN

Los métodos investigativos esgrimidos para el presente trabajo investigativo son dos, debido a que la investigación corresponde a una de tipo mixto, disgregándose cualitativa y cuantitativamente, en primer orden tenemos al método de **Análisis e Interpretación Documental (Hermenéutico)**, debido a que analizará diferentes documentos referentes al problema investigativo, este tipo de contrastación en muchos casos se aplica al Derecho; debido a que es una ciencia basada en la interpretación de los hechos; que debe relacionar las normas a los acontecimientos, y comprobarlos a través de los medios probatorios.

En segundo apartado, el método de la investigación será ***explicativo***, porqué establecerá y explicará las causas por las que el derecho a la intimidad de los usuarios de Internet, debe ser protegido por la legislación nacional en un marco normativo específico a las aplicaciones de Internet, para ello se ha implementado una encuesta que

será aplicada, a cada uno de los sujetos de investigación, los cuales serán seleccionados de manera aleatoria siendo en total 203.

4.5 POBLACION Y MUESTRA

En cuanto a la determinación y elección de la población y muestra, se tomará en consideración, el **muestreo probabilístico**, debido a que la muestra se seleccionará de acuerdo a las fórmulas estadísticas que determinarán, sobre quienes aplicar el instrumento preparado por el investigador, recolectando datos por un lado de los usuarios en contraste con la realidad y por otro lado, de las aplicaciones más representativas de Internet en lo concerniente al derecho fundamental de la intimidad.

4.5.1 Población

En relación a la determinación de la población, se tomará en cuenta a la que accede a Internet, según la Encuesta Nacional de Hogares realizada por el Instituto Nacional de Estadística e Informática, donde se midió la cantidad de usuarios o personas que acceden a Internet según ámbito geográfico y cuya temporalidad corresponde a los años 2007-2013, dicha encuesta dio como resultado que el 44.9% de Arequipeños accede a Internet, porcentaje que se tomará en consideración para la determinación de la muestra, extrapolando dicho porcentaje a la realidad poblacional del distrito de Paucarpata.

4.5.2 Muestra

Dentro de la delimitación espacial dentro de la que se circunscribe el presente trabajo, se ha designado al distrito de Paucarpata como la población de la que se extraerá la muestra, para ello el distrito de Paucarpata presenta una densidad poblacional de 4031.4 habitantes por kilómetro cuadrado y una cantidad de 125255 habitantes, con una tasa de crecimiento del 2%; establecido lo anterior, se determinará el tamaño de la muestra para poblaciones finitas.

Determinando el número de elementos con los que debemos calcular la muestra, se procederá a extraer el 44.9% de los 125255 habitantes en función a la capacidad de acceder a Internet:

Siendo 125255 el total de habitantes de Paucarpata y se necesita el 44.9% que son los que acceden a Internet, por regla de tres simple, se obtiene que el total de la población que accede a Internet del distrito de Paucarpata es: 56239.495

Aplicando la fórmula para determinar la muestra tenemos:

$$N=\frac{Z_{\forall}^{2} * p * q * n}{e^{2}(n-1) + Z_{\forall}^{2} p * q}$$

Dónde:

n = Es el tamaño total de la población.

$\forall$ = Riesgo o nivel de significación.

$Z_{\forall}$ = Puntuación correspondiente al riesgo.

P = Es la probabilidad a favor.

q = Es la probabilidad en contra.

e = Error permitido.

N = Representa el tamaño de muestra.

Reemplazando datos para este caso en particular:

n = 56239.495

$\forall$ = 5

$Z_{\forall}$ = 1.96 redondeando 2

P = 50

q = 50

e = 7

N = ¿...?

$$N=\frac{4*50*50*56239.495}{49(56239.495-1)+4*50*50}$$

N= 203.4

De la formula anterior obtenemos nuestra muestra, que corresponde a 203 personas a las que se aplicará el instrumento.

En explicación a lo anterior, la presente investigación tendrá una muestra de la población del distrito de Paucarpata, de un Universo que estará constituido por personas de ambos sexos que acceden a Internet.

4.6 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

4.6.1 Técnicas

La técnica elegida para el presente trabajo de investigación, es la de ***acopio y análisis documental***, la cual consistirá en la recolección de bibliografía documental (libros, revistas, publicaciones de Internet, legislación nacional e internacional) para realizar un cuadro de análisis e interpretación documental.

Para realizar el análisis documental, en primer lugar se utilizó como instrumento la ficha de Análisis documental, la misma que contiene como características de análisis documental la explicitación del tema, el cual está dirigido a identificar si el documento habla en forma directa al tema abordado, una segundo aparatado está diseñado hacia la concreción de lo señalado en nuestra realidad es decir si se asemeja o difiere completamente de lo presentado en nuestra realidad.

En adición a lo referido anteriormente, y dentro de la técnica de análisis documental, se utilizó la técnica del

Muestreo No Probabilístico Intencional u Opinativo, **(Pantigoso Bustamante, 2011)**, "***donde el investigador selecciona de modo directo los elementos (...) que desea participen en su estudio.*** (...). Se sigue un criterio establecido por el experto o investigador", que para el presente caso son diferentes aplicaciones de Internet que el investigador escogió, atendiendo diferentes criterios que se considera pertinentes, entre ellos, la representatividad social.

En segundo lugar se utilizó la técnica de ***La Encuesta*** lo cual corresponde al trabajo de campo, la cual estuvo dirigida a los usuarios de Internet. Consecuentemente se realizó el acopio de información, para tener una visión más amplia sobre el problema y así contrastarlo con la realidad local para esbozar posibles soluciones.

4.6.2 Instrumentos

A. **Procedimiento de Análisis y Observación Documental,** en primer lugar se analizarán diversas fuentes de información, seleccionando, describiendo, organizando y analizando, la información necesaria sobre la política informática de privacidad, referente a la intimidad y el panorama de vulneración generado por algunas aplicaciones de Internet. En segundo lugar "El análisis de los datos, resulta ser: un conjunto de manipulaciones, transformaciones, operaciones, reflexiones, comprobaciones que se realiza, con el fin de extraer significados relevantes en relación con un problema de investigación, llevado a cabo generalmente preservando su naturaleza textual, poniendo en práctica tareas de categorización y sin recurrir a las técnicas estadísticas" **(Mayz Díaz, 2010, pág. 12)**.

B. La encuesta: el instrumento que se utilizo es el cuestionario, el cual consta de 5 preguntas de opción múltiple, dirigido a los diferentes usuarios que navegan en Internet, debido a la accesibilidad y continuo uso de la red usando alguna aplicación, pues ellos son los sujetos (usuarios) de los derechos que se ven vulnerados y que es materia del presente estudio, además de ser muy factible en ellos la aplicación del instrumento por su aleatoriedad y disposición de tiempo.

MATRIZ DE INSTRUMENTO DE INVESTIGACIÓN

Variable	Dimensión	Indicador	Ítems – sub-indicador
Independiente			
Aplicaciones de Internet	Usuario de Internet	Vulneración	***¿De qué manera considera Ud. que se vulnera su derecho a la intimidad en las aplicaciones de Internet?*** a) Análisis de información íntima b) Registro de comunicaciones. c) Limitaciones al derecho de defensa. d) Cambio de las políticas de privacidad. e) Por Espionaje
Dependiente			
Derecho a la intimidad	Autodeterminación informativa	Manejo de información	***¿Conoce Ud. el tratamiento que realizan con sus datos íntimos las aplicaciones de internet?*** a) Destino desconocido de la información. b) Uso de información íntima. c) Control desigual de la información. d) Beneficio económico con datos íntimos. ***¿Cómo considera Ud. que son recogidos y almacenados sus datos íntimos por las aplicaciones de Internet?*** a) A través de perfiles de navegación online. b) Tráfico de datos. c) Registros obligatorios. d) A través de cuentas de internet.
		Formas de protección	***¿De qué forma cree Ud. que se garantice el derecho a la intimidad en las aplicaciones de Internet?*** a) Respetando la normativa nacional b) Solicitando su consentimiento expreso ***¿Qué tipos de protección a la intimidad le***

			gustaría que implementen las aplicaciones de Internet para sus usuarios? a) Derecho al olvido b) Derecho de cancelación c) Notificar y retirar información d) Reparación de daños causados en Internet e) Avisos de intromisiones.

4.6.3 Criterios de Validez y confiabilidad de los instrumentos

En lo concerniente a validez y confiabilidad del presente instrumento, se puede detallar que se ha utilizado *el juicio de expertos,* para dotar al presente instrumento, de correcciones sobre las posibles fuentes de error. De esta forma los ítems o preguntas han sido corregidas, en base a los tres criterios de los expertos, en conclusión el instrumento ha tenido una impresión de calidad y confiabilidad.

Explicando el proceso de realización y validación del instrumento, se sometió el mismo al sistema de ***juicio de expertos,*** el cual consta de lo siguiente:

a) Se eligieron tres jueces o expertos, los cuales de acuerdo a su lógica y experiencia juzgarán de manera independiente los ítems del instrumento, calificándolo en función a tres criterios:

- **Claridad.**
- **Congruencia.**
- **Tendenciosidad.**

b) Una vez elegidos los tres jueces o expertos, se les entregará la ficha de validación con los tres criterios, para que evalúen dicho instrumento. En este caso se eligió a los siguientes abogados:

- Al docente y abogado ***Luis Jordán Parra,*** con el cargo de Docente de la Escuela de Derecho en la Universidad Alas Peruanas en el curso de Derecho Constitucional.
- A la docente y abogado ***Maribel Acosta Guillen,*** con el cargo de Docente de la Escuela de Derecho en la Universidad Alas Peruanas en el curso de Derecho Constitucional.

- Al docente y abogado ***Omar Candia Aguilar,*** con el cargo de Docente de la Escuela de Derecho en la Universidad Alas Peruanas en el curso de Derecho Constitucional.

c) Los jueces procedieron, en su calidad de expertos, a evaluar el instrumento en base a los criterios señalados, se recogieron los resultados de la evaluación y se analizaron las coincidencias y desacuerdos. Los ítems validados solo parcialmente y los excluidos fueron nuevamente reformulados y presentados para la nueva validación por los jueces.

Ítem	Congruencia		Claridad		Tendenciosidad	
	Si	No	Si	No	Si	No
1	*		*			*
2	*		*			*
3	*		*			*
4	*		*			*
5	*		*			*

d) Se procedió a la sumatoria de cada ítem que calificó cada juez.

Ítem	Congruencia		Claridad		Tendenciosidad	
	Si	No	Si	No	Si	No
1	A		A			A
2	A		A			A
3	A		A			A
4	A		A			A
5	A		A			A

Donde A significa Aprobado o incluido.

e) Se procede a la aplicación de la fórmula de AIKEN.

APLICACIÓN DE LA FÓRMULA	SOLUCIÓN
$V = \frac{S}{(\mathrm{N}(\mathrm{C}-1))}$ S: sumatoria de jueces	$\mathrm{V} = \frac{3}{3(2-1)}$

N: número de jueces C: constituye el número de valores de la Escala en este caso 2 (acuerdo y desacuerdo)	$V = 1$

f) Se analizan los ítems, modos de cuantificación de la respuesta elección múltiple.

a) 0: error.

b) 1: acierto.

Omisión: se puede tratar como error (0) o como no válida.

CAPÍTULO V
ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

5.1 ANALISIS DE DATOS

5.5.1. Elaboración del cuestionario de preguntas.

En este apartado, se referirá el análisis e interpretación de los datos obtenidos del instrumento aplicado, de manera probabilística y aleatoria a 203 personas usuarias de Internet, en el distrito de Paucarpata, provincia y departamento de Arequipa.

Tabla Nº 1

¿De qué manera considera Ud. que se vulnera su derecho a la intimidad en las aplicaciones de Internet?

ALTERNATIVA	f	%
a) Análisis de información íntima	99	49,00
b) Registro de comunicaciones	19	9,00
c) Limitaciones al derecho de defensa	20	10,00
d) Cambio de las políticas de privacidad	26	13,00
d) Por Espionaje	39	19,00
Total	203	100,0%

Fuente: Elaboración del cuestionario sobre las aplicaciones de Internet y el derecho fundamental a la intimidad.

Descripción: De la pregunta bajo análisis se puede colegir que la mayoría de personas considera que su derecho a la intimidad es vulnerado cuando las aplicaciones de Internet analizan su información íntima, ello representa un 49% siendo esta cantidad la que mayor representatividad se ha obtenido de la muestra, seguido a este resultado, otra cantidad representativa de la encuesta revela que el espionaje, es segunda forma como se vulnera su derecho a la Intimidad y por ello se obtuvo un 19%, en tercer lugar aparece con un 13% de personas encuestadas que señalan que su derecho a la intimidad es vulnerado cuando cambian las políticas de privacidad, en cuarto lugar, el 10% de las personas encuestadas sienten limitaciones en su derecho de defensa, considerando ello, una forma de vulneración a su derecho a la intimidad, por último, el 9% de los encuestados señala, que las empresas que brindan sus aplicaciones en Internet vulneran su derecho a la intimidad por medio del registro de sus comunicaciones en las mencionadas aplicaciones.

Interpretación: Mediante los resultados antes descritos, se ha probado, que la principal forma de vulneración a la intimidad en las aplicaciones de Internet se da fundamentalmente, cuando las empresas que brindan aplicaciones en Internet, ya sean estas gratuitas o de pago,

analizan la información íntima de los usuarios, sin dar cabida a una negociación o alguna opción que permita al usuario proteger su información que considere íntima, esto responde a que la mayoría de personas encuestadas se identificó con este ítem respecto a la vulneración de su intimidad, esta respuesta reforzaría la idea planteada en la hipótesis de ser necesaria la implementación de una norma específica para regular las aplicaciones de Internet específicamente en lo correspondiente a la intimidad, en relación no solo a la privacidad sino a la protección de datos ya regulada pero sin relación al tema abordado (las aplicaciones de Internet) un segundo punto a resaltar es el tema referido al espionaje que se da en Internet, frente al cual el ciudadano se siente protegido, ya que estos actos pasan inadvertidos tanto para las aplicaciones de Internet como para una parte de nuestra legislación en concreto, por último un parte de la población siente que al cambiar las políticas de privacidad vulnera su derecho a intimidad, ello debido a que la mayoría de aplicaciones de Internet cambia unilateralmente y sin explicación debida la mencionadas políticas del servicio, por lo tanto de algún modo se obliga al usuario a aceptar las nuevas condiciones de servicio, de tal modo que dichas condiciones solo señalan algunos beneficios, mas no refieren temas como el almacenamiento de los datos y el tratamiento que se hace con ellos.

Gráfico Nº 1

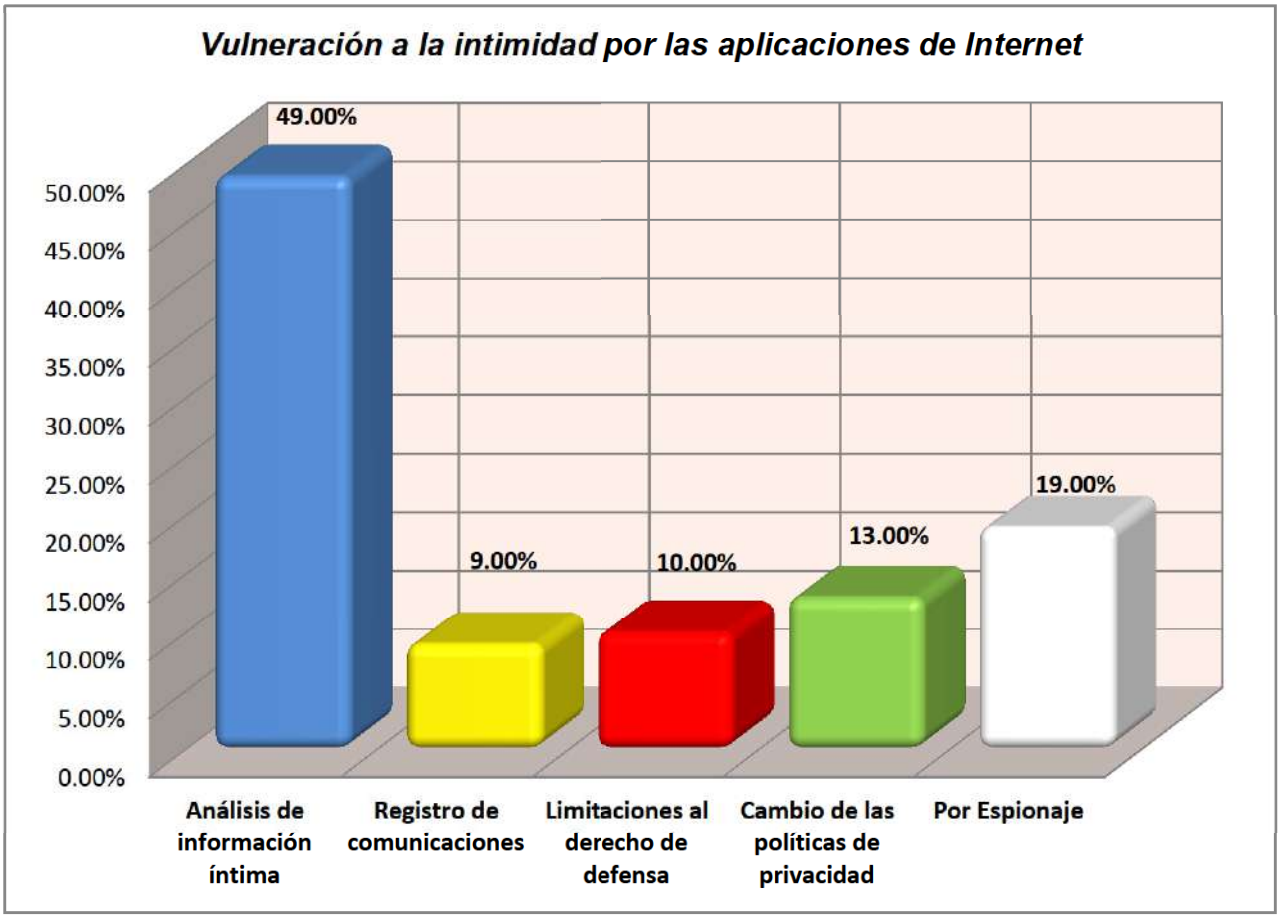

Vulneración a la intimidad por las aplicaciones de Internet
50.00%
45.00%
40.00%
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
49.00%
9.00%
10.00%
13.00%
19.00%
Análisis de información íntima
Registro de comunicaciones
Limitaciones al derecho de defensa
Cambio de las políticas de privacidad
Por Espionaje

Tabla Nº 2

¿Conoce Ud. el tratamiento que realizan con sus datos íntimos las aplicaciones de internet?

ALTERNATIVA	f	%
a) Beneficio económico con datos íntimos	28	14,00
b) Uso de información íntima.	33	16,00
c) Control desigual de la información.	18	9,00
d) Destino desconocido de la información	124	61,00
Total	203	100,0%

Fuente: Elaboración del cuestionario sobre las aplicaciones de Internet y el derecho fundamental a la intimidad.

Descripción:, de una muestra compuesta por 203 personas, se obtuvieron los siguientes datos; se puede relatar que el mayor porcentaje de las personas encuestadas, desconoce el destino de la información que está contenida en las diferentes aplicaciones de Internet obteniendo un 61%, en segundo lugar otra parte considerable de encuestados refiere que las aplicaciones de Internet usan su información íntima obteniendo un 16%, seguido a este resultado, un 14% señala que las diversas aplicaciones de Internet obtienen un beneficio económico de los datos de estas, por último las personas consideran que existe un control desigual de la información que maneja, siendo este resultado el que menos porcentaje obtuvo con un 9% del total de encuestados.

Interpretación: de los datos obtenidos podemos colegir la siguiente glosa; en atención a que el mayor porcentaje de las personas encuestadas, desconoce el destino de la información que está contenida en las diferentes aplicaciones de Internet, obteniendo un 61%, de lo anterior se puede establecer que existe un desconocimiento en este punto de las personas encuestadas en relación al tema propuesto, ello comprueba y refuerza la idea de la hipótesis planteada, pues las diversas aplicaciones de Internet que ofrecen servicios o aplicaciones tanto gratuitos como de pago, en ninguna parte de sus políticas de privacidad o condiciones y términos de servicio, señalan hacia donde se direccionarán

los datos de los usuarios, en qué condiciones se almacenarán o recogerán y si estos serán de algún modo utilizados por la empresa prestadora de alguna aplicación de Internet, por ello se hace patente la idea de regular este punto en una norma específica, tal como se propuso en la hipótesis, en segundo lugar y no muy falto de importancia, otra parte de los encuestados refiere que las aplicaciones de Internet usan su información íntima, en consecuencia, a partir de esta información que el usuario considera sensible o íntima se produce una vulneración a su derecho a la Intimidad, en razón de que una aplicación conoce todo lo referente a los usuarios que usan la misma, pues estos, son conscientes de que aportan demasiada información, a lo que nuestro sistema normativo presta silencio, otro punto a resaltar es el referido beneficio económico que obtienen las aplicaciones de Internet de los datos íntimos tales como patrones de los usuarios, sus gustos, preferencias entre otros que caracterizan y hacen única a la persona y por tanto dicha información solo le concierne a ella, en este orden de ideas, por que las empresas que brindan aplicaciones de Internet no hacen participar a las personas de las que hacen uso de sus datos íntimos en una parte de la ganancia que obtienen o de algún beneficio que contra preste este desprendimiento de algo muy preciado por el usuario, es en este punto donde aparece nuevamente la idea propuesta en la hipótesis pues que mejor que tocar el tema jurídicamente a través de una norma, es claro que el usuario sería una parte de los beneficiados y la otra sería la empresa que a través de incentivos (regulados en una norma) obtenga mayores ganancias que haciéndolo desde las sombras o al margen de la norma.

Gráfico Nº 2

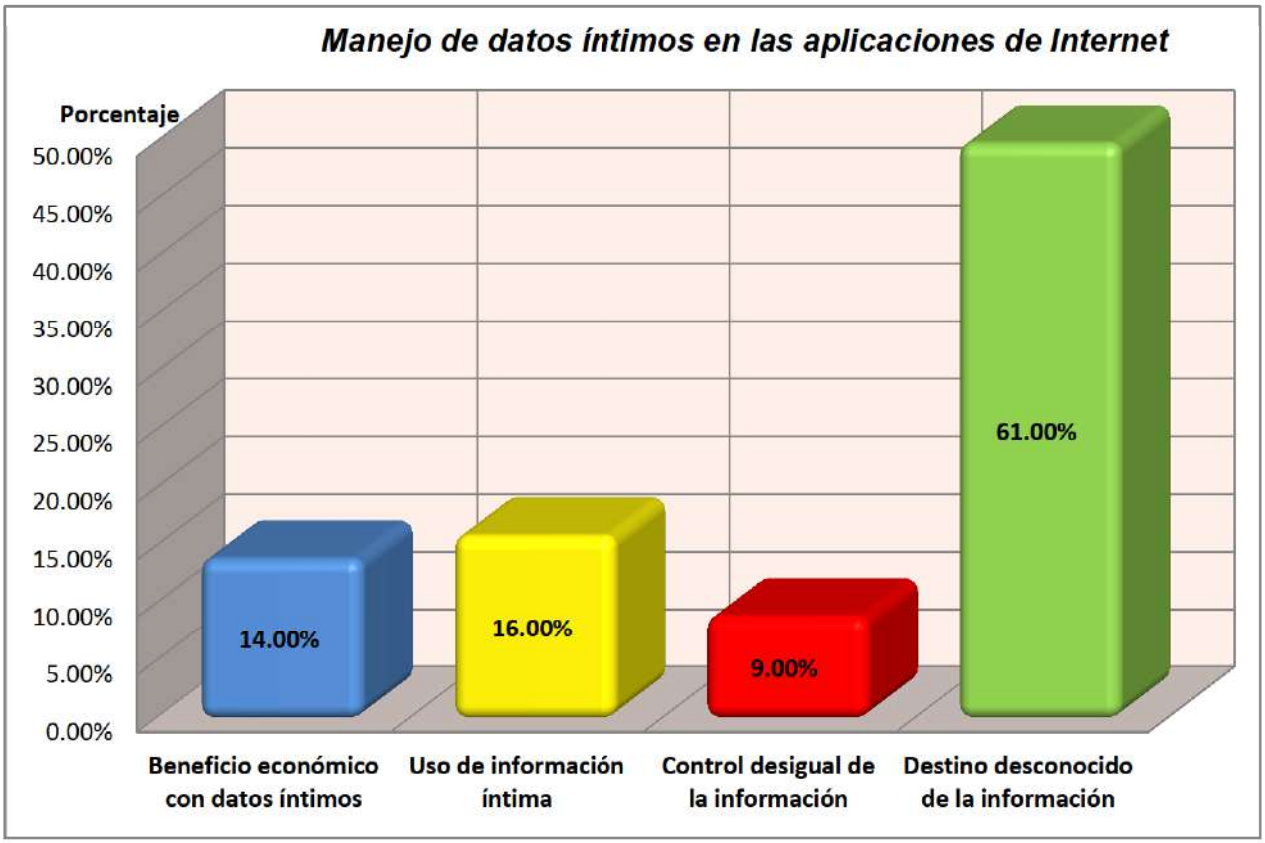

Manejo de datos íntimos en las aplicaciones de Internet
Porcentaje
50.00%
45.00%
40.00%
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
14.00%
16.00%
9.00%
61.00%
Beneficio económico con datos íntimos
Uso de información íntima
Control desigual de la información
Destino desconocido de la información

Tabla Nº 3

¿Cómo considera Ud. que son recogidos y almacenados sus datos íntimos por las aplicaciones de Internet?

ALTERNATIVA	f	%
a) A través de perfiles de navegación online	57	28,00
b) Tráfico de datos	89	44,00
c) Registros obligatorios	15	7,00
d) A través de cuentas de internet	42	21,00
Total	203	100,0%

Fuente: Elaboración del cuestionario sobre las aplicaciones de Internet y el derecho fundamental a la intimidad.

Descripción: los datos obtenidos, de una muestra de 203 personas, señalan que la mayoría de estas, considera que sus datos íntimos son recogidos y almacenados haciendo uso del tráfico de datos de las diferentes aplicaciones de Internet consiguiendo un valor de 44% del total, seguido a ello el 28% de los encuestados manifiesta que las aplicaciones de Internet recogen y almacenan sus datos íntimos a través de los perfiles de navegación online, un menor valor obtuvieron los encuestados que señalaron que dicho recojo y almacenamiento de datos íntimos se realizaba a través de las diversas cuentas de Internet con un total del 21%, por último, un pequeño sector de las personas encuestadas refiere que el recojo y almacenamiento de datos íntimos se realiza a través de los registros obligatorios que presentan algunas aplicaciones en Internet para acceder a sus servicios siendo el valor obtenido el 7% del total.

Interpretación: Por medio del instrumento bajo análisis se ha podido obtener que el ítem que mayor impacto ha tenido en la muestra encuestada, es el tráfico de datos íntimos que realizan las aplicaciones que prestan servicios o aplicaciones en Internet, al parecer las personas notan que las diversas aplicaciones de Internet intercambian información y les ofrecen asombrosamente ofertas pronosticando sus necesidades, al hacer una relación de esta información con la hipótesis planteada se puede afirmar que se comprueba la misma, en el sentido de que se hace

necesaria una norma específica para regular este hecho que constituye el tráfico de datos o como la ley de protección de datos personales señala "flujo transfronterizo de datos", cuando los datos salen y se usan en otro país que para el presente caso sin poder impedirlo o no, ello para concordar el tema con la legislación vigente, sin embargo solo se trata de aplicaciones que se encuentren dentro de nuestro ámbito territorial, de lo cual se hace énfasis al señalar que la mayor concentración de población que hace uso de Internet por medio de una aplicación son los buscadores y las redes sociales, siendo estos dos ejemplos casos en los que no se puede aplicar la mencionada norma de protección de datos personales, de otro lado se ha comprobado que los perfiles de navegación online significan para la población, la forma en como manejan los datos íntimos de los usuarios las diversas aplicaciones de Internet, en consecuencia, se vulnera su derecho a la Intimidad, es por ello que una aplicación conoce todo lo referente a los usuarios que usan la misma, ya que aportan demasiada información (de forma consciente o no), a lo que nuestro sistema normativo presta silencio, por último otro punto a resaltar es el referido al recojo y almacenamiento de datos que se hallan en las diversas cuentas de los usuarios en Internet a lo cual nuevamente se debe señalar que nuestra norma se halla cruzada de brazos ante aplicaciones que se hallan fuera de nuestro país sin poder hacer uso de derechos que deberían poder aplicarse como es el caso de los derechos ARCO[17], sin embargo, la realidad juega con otra moneda.

---

[17] *Derechos ARCO :*
A = Acceso
R = Rectificación
C = Cancelación
O = Oposición

Gráfico Nº 3

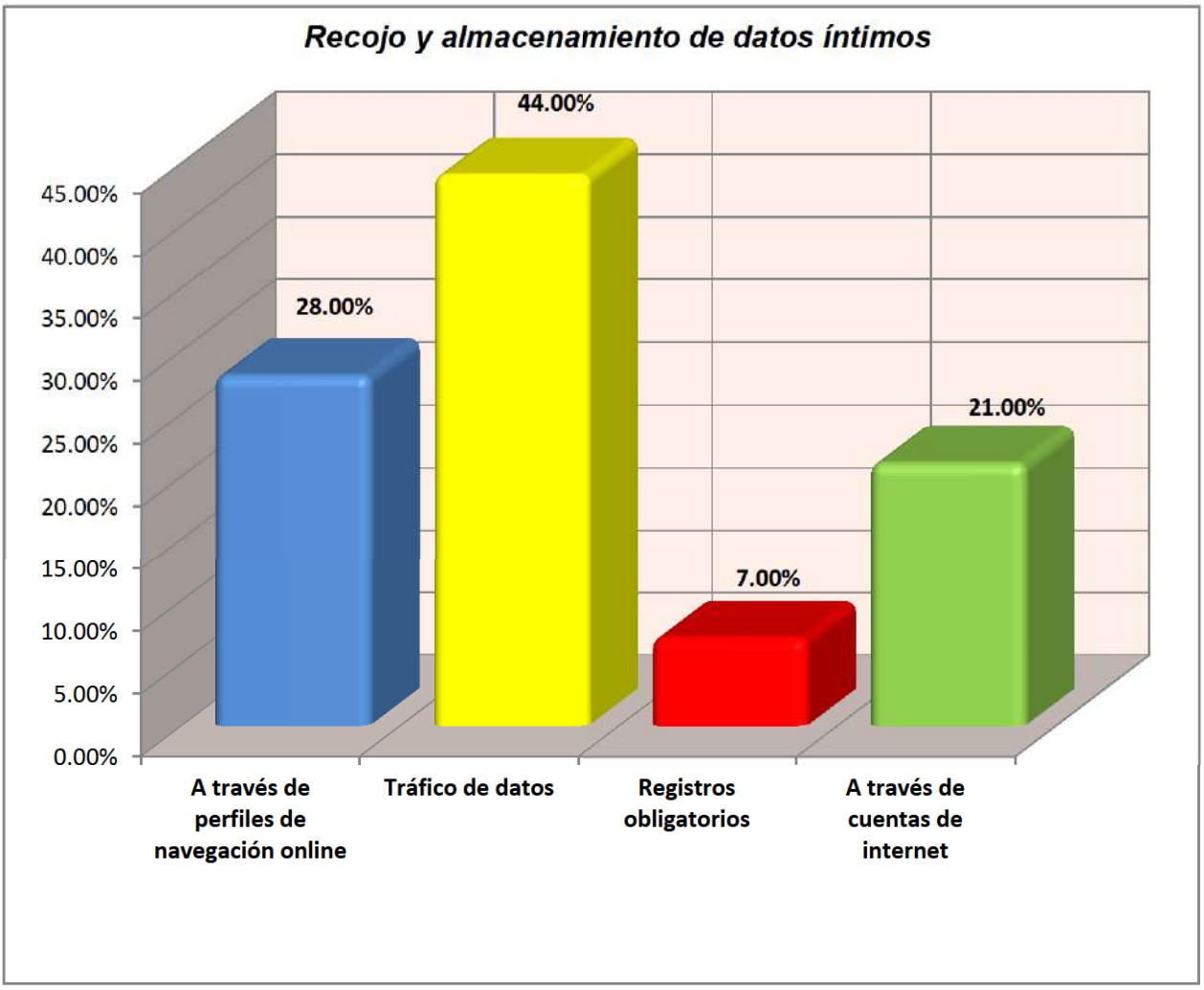

Recojo y almacenamiento de datos íntimos
45.00%
40.00%
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
28.00%
44.00%
7.00%
21.00%
A través de perfiles de navegación online
Tráfico de datos
Registros obligatorios
A través de cuentas de internet

Tabla Nº 4

¿De qué forma cree Ud. que se garantice el derecho a la intimidad en las aplicaciones de Internet?

ALTERNATIVA	f	%
a) Respetando la normativa nacional	119	59,00
b) Solicitando su consentimiento expreso	84	41,00
Total	203	100,0%

Fuente: Elaboración del cuestionario sobre las aplicaciones de Internet y el derecho fundamental a la intimidad.

Descripción: En relación al reactivo planteado a la muestra, el 59% señala que las aplicaciones de Internet deben respetar la normativa nacional, mientras que el restante 41% señala que se le debe solicitar su consentimiento expreso para respetar o garantizar su derecho a la intimidad.

Interpretación: la pregunta en cuestión, esboza un aspecto muy importante en términos jurídicos, pues revela que las aplicaciones de Internet deben respetar la normativa peruana, no solo a razón del legislador, sino porque representa un sentir de la población para que de esta manera se garantice y proteja el derecho a la Intimidad, ello comprueba que la mayoría de las aplicaciones de Internet, necesitan de una normativa específica en nuestro país, que regule y proteja la intimidad de sus usuarios así como la privacidad y la protección de sus datos personales.

Gráfico Nº 4

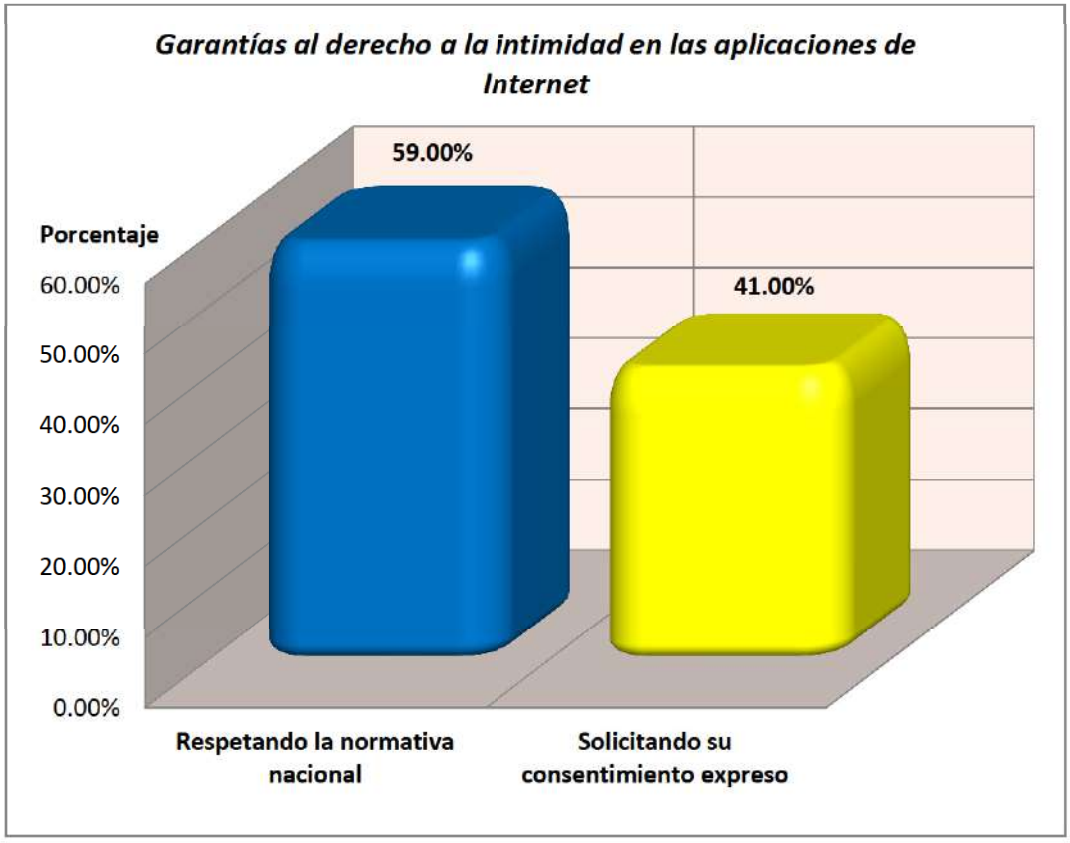

Garantías al derecho a la intimidad en las aplicaciones de Internet
Porcentaje
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
59.00%
41.00%
Respetando la normativa nacional
Solicitando su consentimiento expreso

Tabla Nº 5

¿Qué tipos de protección a la intimidad le gustaría que implementen las aplicaciones de Internet para sus usuarios?

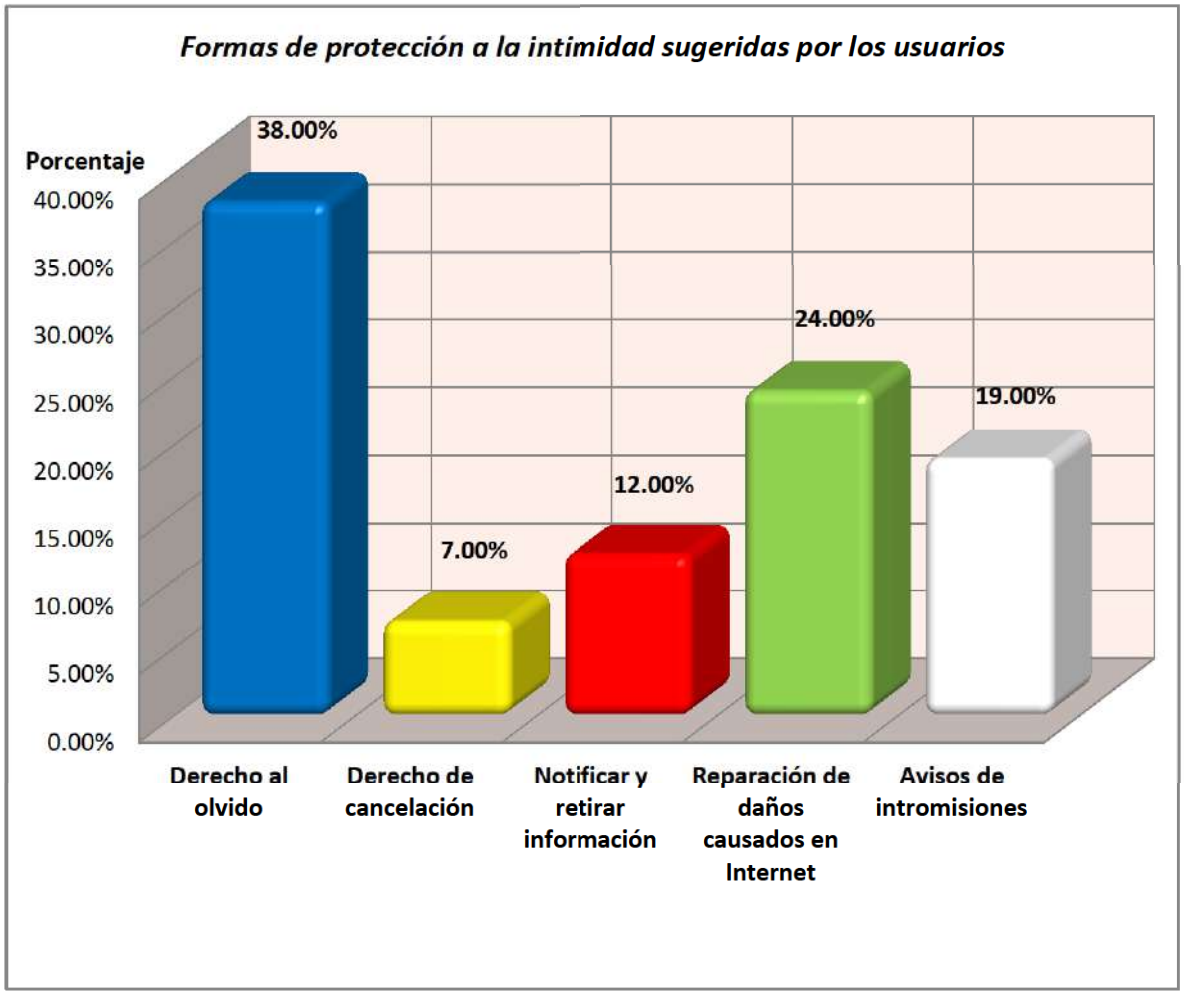
ALTERNATIVA	f	%
a) Derecho al olvido	77	38,00
b) Derecho de cancelación	14	7,00
c) Notificar y retirar información	25	12,00
d) Reparación de daños causados en Internet.	48	24,00
e) Avisos de intromisiones.	39	19,00
Total	203	100,0%

Fuente: Elaboración del cuestionario sobre las aplicaciones de Internet y el derecho fundamental a la intimidad.

Descripción: En primer lugar se observa que el 38% de la muestra hace referencia al derecho al olvido como su forma efectiva de protección a la intimidad que deberían implementar las aplicaciones de Internet, en segundo lugar el 24% de la población señala que debe repararse los daños causados a la intimidad por las aplicaciones Internet, en tercer lugar el 19% expresa que se debe implementar un sistema de aviso de intromisiones en sus datos íntimos, en cuarto lugar el 12% piensa que debe implementarse el sistema de notificación y retiro de la información, por último, el 7% cree que su derecho a la intimidad se haría efectivo por medio del derecho a poder cancelar su información.

Interpretación: De los datos se infiere que la población cree que el derecho al olvido es la mejor forma de protección a su derecho a la intimidad, es válido señalar que la reparación de daños causados en Internet es otra expectativa fuertemente considerada, ambas opciones refuerzan la idea planteada en la hipótesis sobre la necesidad de regular las aplicaciones de Internet con un marco normativo específico, que para este caso añada innovaciones como el derecho al olvido principalmente y la reparación de daños en Internet, implementando nuevas formas de protección a la intimidad que debería regularse a través de una ley, en coordinación con las aplicaciones que brinden servicios en Internet.

Gráfico Nº 5


Formas de protección a la intimidad sugeridas por los usuarios
Porcentaje
40.00%
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
38.00%
7.00%
12.00%
24.00%
19.00%
Derecho al olvido
Derecho de cancelación
Notificar y retirar información
Reparación de daños causados en Internet
Avisos de intromisiones

5.2 PRUEBA DE HIPÓTESIS

De la primera pregunta formulada en el instrumento de recojo de datos, referida a la vulneración de la intimidad en las aplicaciones de Internet los encuestados señalaron con mayor énfasis el ítem que corresponde al análisis de la información íntima de los usuarios, sin dar cabida a una negociación o alguna opción que permita al usuario proteger su información que considere íntima, esta respuesta reforzaría la idea planteada en la hipótesis de ser necesaria la implementación de una norma específica para regular las aplicaciones de Internet específicamente en lo correspondiente a la intimidad, en relación no solo a la privacidad sino a la protección de datos ya regulada pero sin relación al tema abordado (las aplicaciones de Internet)

De la segunda pregunta la mayoría de personas encuestadas, desconoce el destino de la información que está contenida en las diferentes aplicaciones de Internet, este resultado permitió comprobar la idea de la hipótesis planteada, pues las diversas aplicaciones de Internet que ofrecen servicios o aplicaciones tanto gratuitas como de pago, en ninguna parte de sus políticas de privacidad o condiciones y términos de servicio, señalan hacia donde se direccionarán los datos de los usuarios, en qué condiciones se almacenarán o recogerán sus datos y si estos serán de algún modo utilizados por la empresa prestadora de alguna aplicación de Internet, por ello se hace patente la idea de regular este punto en una norma específica, tal como se propuso en la hipótesis.

En cuanto a la tercera pregunta del instrumento de recojo de datos la respuesta que mayor impacto ha tenido en la muestra encuestada, es el tráfico de datos íntimos que realizan las aplicaciones que prestan servicios o aplicaciones en Internet, punto que refuerza la tesis planteada en el sentido de que existe una creciente necesidad de regular a través de una norma específica el tráfico de datos que realizan algunas aplicaciones

de Internet, más aún cuando nuestra población hace mayor uso de aplicaciones que manejan datos íntimos cuya sede y banco de datos se halla en otro país.

En relación a la cuarta pregunta resulta evidente que esta pregunta determina y afirma lo propuesto por la hipótesis, al señalar literalmente que la muestra encuestada en su mayoría señala como necesidad que las diversas aplicaciones de Internet se regulen a través de una norma específica más aún cuando estas manejan datos íntimos que las personas consciente o inconscientemente dejan en sus bases de datos.

En último lugar la pregunta número cinco señala que de ser posible una forma de proteger eficientemente la intimidad de las personas es la correspondiente al derecho al olvido, figura que se maneja en la legislación europea y que visto desde el ámbito legal no existe en nuestra marco normativo, ello aún comprueba nuevamente la hipótesis planteada sobre la necesidad de regular el tema de la intimidad en una norma o ley específica.

5.3 DISCUSIÓN DE RESULTADOS

Como resultado de la presente investigación en relación a la necesidad de aplicar un marco normativo específico a las aplicaciones de internet, los tres puntos sobre los que se ha centrado el instrumento de recojo de datos han sido el de la vulneración, manejo de datos y protección de la intimidad, a lo cual, nuestra normativa se encuentra carente de acciones específicas debido a que en la tabla 1 referente a la pregunta ¿De qué manera considera Ud. que se vulnera su derecho a la intimidad en las aplicaciones de Internet?, se generó como respuesta dominante que las mencionadas aplicaciones de Internet vulneran el derecho de los usuarios mediante el análisis que realizan sobre la información íntima de los mismos, ello señala que las aplicaciones en

cuestión, no respetan la normativa nacional a nivel constitucional en derechos como: protección de datos, prohibición de registros obligatorios, responsabilidad civil, tal y como se aprecia en la tabla y gráfico 1, además se puede señalar que esta vulneración a la intimidad guarda relación con el tratamiento de datos analizado en la tabla Nº 2, que realizan las diversas aplicaciones de Internet, ya que el destino de la información del usuario tiene un destino desconocido para el mismo, es sabido que nuestro compendio normativo cuenta con un instrumento legal denominado ley de protección de datos personales, además, si dicho acto es punible se hallaría inserto en los delitos que contempla el código Penal referente a la intimidad de la persona, sin embargo ante temas y supuestos como los planteados en las preguntas bajo discusión, ambas normas se hallan carentes de acción, puesto que por un lado no configurarían un tipo establecido y por el otro estarían fuera del rango de aplicación de la norma, tanto penal como de protección de datos personales, es en este sentido donde cobra fuerza el pensamiento manifestado en hipótesis para el presente trabajo, sobre la necesidad de una norma específica que regule los aspectos propuestos y que coordine acciones tanto con el ámbito penal como con el administrativo, puesto que se tratan de derechos fundamentales que se deben proteger,

De las tablas Nº 1, Nº 2, Nº 3, Nº 4 y Nº 5, se puede inferir que las diversas aplicaciones que ofrecen sus servicios en Internet no permiten negociar u optar al usuario cuando se suscribe en ellas en lo referente a la intimidad, ello en razón en ningún momento se permite al usuario manejar su intimidad, todo lo contrario, la aceptación de determinado servicio pretende extrapolar en ella la cesión de todos los derechos que el usuario pueda exigir o no en favor de la mencionada aplicación, ya que toda la información del usuario es filtrada y analizada (tal y como lo señalado en la tabla 1) por complejos programas que las diversas aplicaciones de Internet empleen, seguido a ello no se hace mención respecto a que datos se emplearan y que otro no o si se hará uso de

todos (tabla Nº 2), tampoco se hace referencia al almacenamiento y destino de la información del usuario, así mismo, no se menciona claramente el uso de programas que recogen los datos del usuario y que harán con ellos, del mismo modo al hacerse alusión a los datos sensibles que determinadas aplicaciones de Internet dejan a criterio del usuario de rellenar al hacer uso de las mismas, por otro lado las diversas aplicaciones de Internet no presentan la opción sobre el uso de la normativa origen del usuario, solo se limitan a decir que al aceptar deben someterse a tal o cual legislación a lo que es taxativa la respuesta optada por los encuestados en el gráfico 4, por último en cuanto a las innovaciones que consideran los usuarios les protegerá mejor su intimidad el derecho al olvido toma especial énfasis, sin embargo el que una aplicación implemente dicho derecho en atención a uno o algunos de sus usuarios no es posible, todo ello, cuando estas denominadas aplicaciones de Internet se conducen a modo anárquico, es decir, sin querer adoptar la legislación del usuario para la cautela de sus derechos.

CAPÍTULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

PRIMERA: Se identificó que el principal uso que realizan las aplicaciones de Internet con los datos íntimos de los usuarios, se da a través del tráfico de datos y el recojo de perfiles de navegación online, pudiendo deducir, que gran parte de los usuarios, considera que su derecho a la intimidad es vulnerado cuando las aplicaciones de Internet analizan su información íntima, afectando de esta manera el derecho a la intimidad de los mismos; asimismo, se expresó el desconocimiento del destino de la información íntima del usuario y sus fines por parte de las diversas aplicaciones de Internet.

SEGUNDA: Se describió, que las principales formas de vulneración a la intimidad son: el análisis de información íntima, el registro de comunicaciones, las limitaciones al derecho de defensa, el constante cambio de las políticas de privacidad y el espionaje realizado por diversas organizaciones, evidenciando de esta manera que la principal forma de vulneración al derecho a la intimidad, es la referida al análisis de la información íntima que realizan determinadas aplicaciones de Internet, sin ningún aviso ni consentimiento pedido al usuario.

TERCERA: Se determinó que dentro de las formas de protección, propuestas para resguardar la intimidad del usuario, el derecho al olvido corresponde a la necesidad que mayor significatividad tiene en la sociedad, porque este novedoso sistema responde en mayor grado a los nuevos avances tecnológicos que utiliza diariamente nuestra población, respecto a las aplicaciones de Internet, además, se determinó que las aplicaciones de Internet deben acatar nuestra normativa nacional para salvaguardar la necesidad de protección que los usuarios plantean.

6.2. RECOMENDACIONES

PRIMERA: Se recomienda al legislador y al operador jurídico, que la mejor forma de esbozar una solución al problema propuesto, en lo concerniente a la obtención, uso y manejo de datos por las aplicaciones de Internet en relación a los usuarios, corresponde a formular un esquema normativo, tomando en cuenta los adelantos que han implementado diversos países en relación a Internet y la intimidad del usuario, para enunciar una ley y brindar soluciones acertadas, definiendo temas discutidos como el propuesto, no en base solo a nuestra realidad, sino a lo que enuncia el porvenir de otras realidades (visión global) que viven y definen problemas en función de las personas que cada vez más hacemos uso de Internet, pues este medio es afín a muchos pueblos, como el nuestro y que más necesita de protección.

SEGUNDA: Se recomienda al legislador, tomar en cuenta la posición brasileña, pues es un claro ejemplo de querer proteger a sus usuarios dotándolos tanto de derechos como obligaciones, que del mismo modo operan para las empresas prestadoras de aplicaciones en Internet, es en razón a ello, que se debe tomar especial atención al momento de crear las normas relativas a Internet, cuyo fin debe ser el bien común, velando por los derechos de los usuarios finales y no permitir su cosificación, situación que no nos diferenciaría de cualquier producto.

TERCERA: Se recomienda al legislador permitir al derecho de nuestro país, considerar y analizar las nuevas realidades tecnológicas, protegiendo los derechos de los usuarios contra posibles situaciones de vulnerabilidad, activamente, en forma flexible, adecuada y que no limite los avances en la materia, es válido recalcar, que nuestras normas deben permitir la creación de añadidos que admitan mayor flexibilidad al cambio, pues este problema al mismo tiempo que abarca un problema nacional tiene una esencia preeminentemente global, siendo así, es evidente que la tecnología de hoy determinará el futuro de nuestras normas.

BIBLIOGRAFÍA

- Aguado, J. (2011). Universidad de Murcia. Recuperado el 17 de 11 de 2014, de www.um.es/tic/Txtguia/Introduccion%20a%20las%20Teorias%20de%20la%20Informa%20(20)/TIC%20texto%20guia%20completo.pdf
- Alonso, J. (30 de 06 de 2011). Evoca Comunicación e Imagen. (J. Cerezo Gilarranz, Ed.) Recuperado el 24 de 10 de 2014, de www.evocaimagen.com
- Alt1040. (19 de 01 de 2012). Recuperado el 18 de 10 de 2014, de http://alt1040.com/2012/01/megaupload-cierra
- Álvarez Rodríguez, L. (2012). IV Foro Internacional Derechos Humanos y Tecnologías de la Información y la comunicación. Recuperado el 27 de 9 de 2014, de Repositorio digital: www.repositoriodigital.ipn.mx/bitstream/handle/123456789/3987/Memoria%204to%20Foro%20DHTIC%2015.pdf?sequence=1
- Arias Bustamante, D. (06 de 2014). Tesis: ADAPTACIÓN DEL PRINCIPIO DE NEUTRALIDAD DE LA RED A LA REALIDAD COSTARRICENSE. Recuperado el 05 de 10 de 2014, de iij.ucr.ac.cr/sites/default/files/documentos/tesis-_adaptacion_del_principio_de_neutralidad_de_la_red_a_la.pdf
- Ávalos, N., & Tapia M, S. (10 de 2013). Scielo.cl. Recuperado el 16 de 07 de 2014, de http://www.scielo.cl/pdf/rchcir/v65n5/art14.pdf
- Basilio Araujo, S., & Samamé Toribio, B. (2008). Monografías.com. Recuperado el 15 de 09 de 2014, de http://www.monografias.com/trabajos65/derecho-intimidad/derecho-intimidad.zip
- Benítez Jiménez, E. (17 de 11 de 2012). Recuperado el 19 de 03 de 2015, de https://elisainformatica.files.wordpress.com/2012/11/aplicaciones-informc3a1ticas.pdf
- Bernales Ballesteros, E. (1999). La constitución de 1993 Análisis comparado. Lima, Perú: EDITORA RAO S.R.L. : Setiembre de 1999.
- Bitelia. (25 de 09 de 2014). Recuperado el 09 de 10 de 2014, de http://bitelia.com/2014/09/tim-berners-lee
- Brian Nougrères, A. (07 de 2012). Habeasdatacolombia. Recuperado el 06 de 07 de 2015, de habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf
- Carbonell, M. (2004). Los Derechos fundamentales en México. México.
- Correo/Agencias. (07 de 06 de 2013). EE.UU. registró en secreto llamadas. Correo, pág. 15.
- Cotino Hueso, L. (2011). La colisión del derecho a la protección de datos personales y las libertades informativas en la red: pautas generales y particulares de solución. En L. Cotino Hueso, Libertades de expresión e información en Internet y las redes

sociales: ejercicio, amenazas y garantías (págs. 386-401). Servei de Publicacions de la Universitat de València.

- Cristos Velasco, S. (03 de 12 de 2004). Recuperado el 26 de 10 de 2014, de http://www.inegi.org.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf
- Dellacasacastillo.com. (2014). Recuperado el 30 de 12 de 2014, de http://www.dellacasacastillo.com/glosario.htm
- Derecho.com. (2014). Recuperado el 30 de 12 de 2014, de http://www.derecho.com/c/C%C3%B3digo_de_conducta
- Derecho.com (A). (2014). Recuperado el 30 de 12 de 2014, de www.derecho.com/c/Derechos_humanos
- Derecho.com (B). (2014). Recuperado el 30 de 12 de 2014, de http://www.derecho.com/c/Derechos_fundamentales
- Díaz Tolosa, R. (2007). Scielo. Recuperado el 10 de 12 de 2014, de http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122007000100011
- Doneda, D. (2014). Recuperado el 17 de 10 de 2014, de www.privacylatam.com/wp-content/uploads/2014/10/Danilo-Doneda_SanAndres141014.pdf
- El blog salmón. (2013). Recuperado el 15 de 11 de 2014, de http://www.elblogsalmon.com/empresas/facebook-vende-la-informacion-personal-de-sus-usuarios
- El rincón del vago. (2004). Recuperado el 12 de 9 de 2014, de html.rincondelvago.com/delitos-informaticos_1.html
- Emparan Legaspi, A. (2012). Estela Digital. Recuperado el 26 de 11 de 2014, de caipec.org.mx/wp-content/uploads/2012/12/Estela-Digital.-Derecho-a-la-privacidad-y-protecci%C3%B3n-de-datos-personales-en-Facebook.-2o.pdf
- Enciclopedia Jurídica. (2014). Recuperado el 24 de 11 de 2014, de http://www.enciclopedia-juridica.biz14.com/d/indefension/indefension.htm
- ESET-Latinoamérica, E. d. (2014). ESET Latinoamérica. Recuperado el 27 de 10 de 2014, de http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf
- Fbclaim. (21 de 07 de 2014). Recuperado el 08 de 08 de 2014, de https://www.fbclaim.com/ui/page/faqs#int
- Francés, G. (2006). El teclas.com. Recuperado el 19 de 11 de 2014, de www.elteclas.com/internet/internet_historia.pdf
- Genbeta. (10 de 11 de 2014). Recuperado el 15 de 11 de 2014, de http://www.genbeta.com/actualidad/obama-la-neutralidad-de-la-red-es-un-principio-esencial-y-hay-que-protegerlo
- Gonzales, A. (2008). aquilinogonzalez.es. Recuperado el 26 de 10 de 2014, de www.aquilinogonzalez.es/IFORMAT4ESO/Unidad_4.pdf

- González Cifuentes, C. (2011). Recuperado el 11 de 01 de 2015, de gredos.usal.es/jspui/bitstream/10366/115568/1/DDPG_Gonzalez_Cifuentes_C._El_derecho.pdf
- Goyzueta, V. (04 de 05 de 2014). La nueva ley brasileña, modelo para la defensa de neutralidad. ABC, págs. 56-57.
- Gutiérrez David, E. (06 de 2013). derecom. Recuperado el 17 de 10 de 2014, de www.derecom.com/numeros/pdf/estrella2.pdf
- Herrán Ortiz, A. (2003). Universidad de Deusto. Recuperado el 26 de 11 de 2014, de www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf
- Herrera de Egaña, J. (04 de 2007). Revista InDret para el análisis del derecho. Recuperado el 19 de 10 de 2014, de www.raco.cat/index.php/InDret/article/download/78573/102649
- Huerta Guerrero, L. (2012). Blog de la Pontificia Universidad Católica del Perú. Recuperado el 30 de 12 de 2014, de http://blog.pucp.edu.pe/item/137301/promulgan-ley-de-proteccion-de-datos-personales-ley-n-29733
- Huerta Moreno, M. (2005). Redalyc. Recuperado el 3 de 10 de 2014, de http://www.redalyc.org/pdf/267/26702406.pdf
- Klink, T. (2011). La actual posición del Tribunal Supremo alemán ante la libertad de expresión en la red, el caso de la "chuleta" – "spickmich.de". En L. Cotino Hueso, Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías (págs. 88-98). Servei de Publicacions de la Universitat de València.
- La Constitución Comentada. Gaceta Juridica S.A. (2005).
- López Herrera, E. (10 de 2004). Universidad Nacional de Tucumán. Recuperado el 19 de 11 de 2013, de www.derecho.unt.edu.ar/publicaciones/Introdresponsabilidadcivil.pdf
- López Herrero, M., López Moreno , V., & Galán Martín, E. (2010). Universidad Complutense de Madrid. Recuperado el 26 de 10 de 2014, de www.websatafi.com/joomla/attachments/125_REDES%20SOCIALES%20PUBLICAR.pdf
- Machicado, J. (05 de 2012). Recuperado el 24 de 10 de 2014, de http://jorgemachicado.blogspot.com/2012/05/depe.html
- Martin Gavilan, C. (2009). Recuperado el 02 de 12 de 2014, de http://eprints.rclis.org/14285/1/internet.pdf
- Marty, B. (23 de 04 de 2014). Recuperado el 14 de 12 de 2014, de http://es.panampost.com/belen-marty/2014/04/23/brasil-arranca-en-san-pablo-cumbre-mundial-que-decidira-el-futuro-de-internet/
- Mayz Díaz, C. (2010). Universidad de Carabobo. Valencia, Venezuela. Recuperado el 16 de 12 de 2014, de http://www.scielo.org.ve/pdf/edu/v13n44/art07.pdf

- Mendoza Riofrío, M. (2014). El comercio. Recuperado el 22 de 10 de 2014, de http://elcomercio.pe/economia/negocios/como-se-comportan-usuarios-internet-peru-noticia-1736688
- Ministerio de Justicia y Derechos Humanos. (2014). Recuperado el 29 de 04 de 2014, de www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-Derecho-Fundamentalok.pdf
- Miranda Alcántara, M. (2003). Teleley.com. Recuperado el 26 de 11 de 2014, de www.teleley.com/articulos/art-miranda.pdf
- Miranda Londoño, A. (2000). Pontificia Universidad Javeriana. Recuperado el 22 de 06 de 2014, de www.javeriana.edu.co/biblos/tesis/derecho/dere2/Tesis12.pdf
- Miranda P., H. (25 de 10 de 2014). Diario la Nación. Recuperado el 03 de 11 de 2014, de http://www.nacion.com/sucesos/poder-judicial/Corte-reglas-proteger-sensibles-sentencias_0_1447255299.html
- Navarro Floria, J. (08 de 2012). Universidad Catolica Argentina. Recuperado el 05 de 12 de 2014, de bibliotecadigital.uca.edu.ar/repositorio/contribuciones/derechos-personalisimos-navarro-floria.pdf
- Navas Navarro, S. (03 de 2015). Blog de la Universidad de Castilla-La Mancha. Recuperado el 04 de 04 de 2015, de blog.uclm.es/cesco/files/2015/03/La-personalidad-virtual-del-usuario-de-internet-.pdf
- ONGEI. (2014). Oficina Nacional de Gobierno Electrónico. Recuperado el 2014, de http://www.ongei.gob.pe/quienes/ongei_QUIENES.asp
- Orrego, C. (2014). Corte Interamericana de Derechos humanos. Recuperado el 23 de 12 de 2014, de http://www.corteidh.or.cr/tablas/r32202.pdf
- Ortiz Gaspar, D. (2012). Derecho y cambio social. Recuperado el 15 de 12 de 2014, de www.derechoycambiosocial.com/revista031/acceso_a_la_informacion_publica.pdf
- Pantigoso Bustamante, V. (2011). La investigación científica y la elaboración de la tesis en Derecho. Arequipa.
- Piñar Mañas, J. (Ed.). (2005). AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Recuperado el 26 de 04 de 2014, de https://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf
- Pisanty Baruch, A. (25 de 09 de 2012). Recuperado el 2014 de 10 de 26, de www.sre.gob.mx/revistadigital/images/stories/numeros/n79-80/pisanty.pdf
- Poire, M. (30 de 04 de 2014). Mediatizada.com. Recuperado el 17 de 10 de 2014, de http://www.mediatizada.com.ar/brasil-aprobo-el-marco-civil-de-internet/
- Puyol, J. (16 de 03 de 2015). Ecix Group. Recuperado el 19 de 03 de 2015, de http://ecixgroup.com/el-grupo/una-aproximacion-juridica-al-concepto-de-neutralidad-tecnologica/
- Raiteri, R. (2011). Techtear. Recuperado el 04 de 08 de 2014, de http://tech.batanga.com/2011/05/13/%C2%BFque-es-una-aplicacion-online

- Revoredo, A. (14 de 10 de 2013). Recuperado el 28 de 10 de 2014, de www.blawyer.org/2013/10/14/adolescentes-y-redes-sociales/#more-7968
- Rivera, J. (10 de 2012). Recuperado el 07 de 12 de 2014, de www.derecho.uba.ar/publicaciones/pensar-en-derecho/revistas/0/derechos-y-actos-personalisimos-en-el-proyecto-de-codigo-civil-y-comercial.pdf
- Roig Batalla, A. (2011). Tecnología, libertad y privacidad. En L. Cotino Hueso, Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías (págs. 44-51). Valencia: Servei de Publicacions de la Universitat de València.
- Ros Martin, M. (2010). Documentalista enredado.net. Recuperado el 30 de 12 de 2014, de www.documentalistaenredado.net/contenido/2009/art-ros-redes-sociales.pdf
- Rubio Moraga, Á. (14 de 09 de 2006). Universidad Complutense de Madrid. Recuperado el 19 de 11 de 2014, de pendientedemigracion.ucm.es/info/hcs/angel/articulos/historiaeinternet.pdf
- s/a. (2001). Universidad de Los Andes. Recuperado el 11 de 12 de 2014, de www.saber.ula.ve/bitstream/123456789/16567/1/internetcomunicacion.pdf
- s/a. (2005). Derechos Humanos Manual para Parlamentarios. Francia.
- s/a. (02 de 07 de 2013). conocimientosweb.net. Recuperado el 26 de 11 de 2014, de http://www.conocimientosweb.net/dcmt/ficha13581.html
- s/a. (16 de 06 de 2014). El Comercio. Recuperado el 06 de 07 de 2014, de http://elcomercio.pe/economia/peru/crece-17-interanual-usuarios-internet-peru-noticia-1736672
- s/a. (26 de 05 de 2015). Foro de la Gobernanza de Internet en España. Recuperado el 28 de 05 de 2015, de www.igfspain.com/doc/archivos/Gobernanza_Internet_Spain_2015.pdf
- s/a. (2015). Universidad de Cambridge. Recuperado el 18 de 03 de 2015, de http://youarewhatyoulike.com/
- s/a. (s.f.). Alegsa.com. Recuperado el 18 de 09 de 2014, de http://www.alegsa.com.ar/Dic/usuario.php
- s/a. (s.f.). Banco Mundial. Recuperado el 15 de 11 de 2014, de http://datos.bancomundial.org/indicador/IT.NET.USER.P2
- s/a. (s.f.). Definicion.de. Recuperado el 18 de 09 de 2014, de http://definicion.de/usuario/
- s/a. (s.f.). Google. Recuperado el 10 de 10 de 2014, de https://sites.google.com/site/plevalenciamkt04/home/aplicaciones-en-internet-1
- s/a. (s.f.). Servicios TIC. Recuperado el 17 de 11 de 2014, de http://www.serviciostic.com/las-tic/definicion-de-tic.html

- s/a. (s.f.). TICs en el aula. Recuperado el 17 de 05 de 2013, de http://ticsenelaula.espacioblog.com/post/2007/11/20/aaque-son-tics
- Webjurídico. (s/f). Recuperado el 16 de 12 de 2014, de http://www.webjuridico.net/hoi/hoi07.htm
- Saltor, C. (2013). Universidad Complutense de Madrid. Recuperado el 17 de 11 de 2014, de eprints.ucm.es/22832/1/T34731.pdf
- Sar Suarez, O. (2013). Recuperado el 26 de 10 de 2014, de www.derecho.usmp.edu.pe/sapere/sumario/primer_bimestre/articulos/Aspectos_sustantivos_procesales_del_Habeas_Data.pdf
- Schubert Gallardo, N. (03 de 2012). Recuperado el 16 de 10 de 2014, de www.fne.gob.cl: www.fne.gob.cl/wp-content/uploads/2014/07/Pre_1%C2%B0_2014.pdf
- Simón Lorda, P., & Concheiro Carroba, L. (20 de 03 de 2014). Researchgate.net. Recuperado el 16 de 07 de 2014, de http://www.researchgate.net/publication/260909012_El_consentimiento_informado_Teora_y_prctica_%28I%29
- Stallman, R. (18 de 11 de 2014). gnu.org. Recuperado el 01 de 12 de 2014, de https://www.gnu.org/philosophy/technological-neutrality.es.html
- Tribunal Constitucional. (2005). Recuperado el 19 de 11 de 2014, de URL: http://www.tc.gob.pe/jurisprudencia/2005/01417-2005-AA.html
- Tribunal Constitucional. (2006). Recuperado el 19 de 11 de 2014, de http://www.tc.gob.pe/jurisprudencia_sistematizada/jurisprudencia_constitucional/dignidad_02273-2005-PHC_FJ10.html
- Tribunal Constitucional B. (2006). Recuperado el 19 de 11 de 2014, de URL: http://www.tc.gob.pe/jurisprudencia/2006/2273-2006-PHC.html
- Tribunal Constitucional. (30 de 04 de 2013). Recuperado el 26 de 11 de 2014, de www.tc.gob.pe/jurisprudencia/2013/01887-2012-HD%20Resolucion.pdf
- Trigo Aranda, V. (s/f). www.acta.es. Recuperado el 19 de 11 de 2014, de www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf
- Universidad de Palermo. (s.f.). Recuperado el 2014 de 10 de 26, de www.palermo.edu/cele/pdf/MODEL-NEUTRALITY
- Vásquez Rocca, L. (2010). Recuperado el 24 de 11 de 2014, de http://www.observacionesfilosoficas.net/fenomenologiadelaintimidad.htm
- Vega Suarez, A. (06 de 2013). Aspectos profesionales. Recuperado el 21 de 06 de 2015, de http://www.aspectosprofesionales.info/2013/06/analisis-del-privacy-by-design-y-su.html
- Viera Lozano, S. (08 de 04 de 2014). Proyecto Fin de Máster. Recuperado el 07 de 02 de 2015, de https://proyectofindemaster.wordpress.com/2014/04/08/la-privacidad-convertida-en-bien-intangible-por-las-redes-sociales/

- VILARROIG, J. (2007). Recuperado el 31 de 10 de 2014, de www.uji.es/bin/publ/edicions/jfi12/18.pdf
- Wikipedia. (2013). Recuperado el 17 de 03 de 2014, de http://es.wikipedia.org/wiki/Indefensi%C3%B3n
- Wikipedia. (2014). Recuperado el 30 de 12 de 2014, de http://es.wikipedia.org/wiki/Neutralidad_de_red
- Wikipedia (B). (2014). Recuperado el 30 de 12 de 2014, de http://es.wikipedia.org/wiki/Usuario_%28inform%C3%A1tica%29
- Wikipedia (C). (2014). Recuperado el 30 de 12 de 2014, de http://es.wikipedia.org/wiki/Derechos_personal%C3%ADsimos
- Wikipedia (D). (2014). Recuperado el 22 de 12 de 2014, de https://es.wikipedia.org/wiki/Supremac%C3%ADa_constitucional
- Wikipedia. (19 de 02 de 2015). Recuperado el 03 de 03 de 2015, de http://es.wikipedia.org/wiki/Derecho_a_la_intimidad
- Wikipedia (B). (2015). Recuperado el 27 de 02 de 2015, de http://es.wikipedia.org/wiki/Derechos_constitucionales
- Wikipedia (C). (2015). Recuperado el 02 de 06 de 2015, de es.wikipedia.org/wiki/Historia_del_estado_del_bienestar
- Zaballos Pulido, E. (2013). UNIVERSIDAD COMPLUTENSE DE MADRID. Recuperado el 16 de 07 de 2014, de eprints.ucm.es/22849/1/T34733.pdf

Anexo 1 A

UNIVERSIDAD "ALAS PERUANAS"

FILIAL AREQUIPA.

ENCUESTA SOBRE LAS APLICACIONES DE INTERNET Y EL DERECHO FUNDAMENTAL A LA INTIMIDAD

Instrucciones: La presente encuesta se ha elaborado con el fin de establecer la importancia del derecho fundamental a la intimidad en las aplicaciones de Internet. Marque solo una respuesta.

---

1. ***¿De qué manera considera Ud. que se vulnera su derecho a la intimidad en las aplicaciones de Internet?***
   a) Análisis de información íntima
   b) Registro de comunicaciones.
   c) Limitaciones al derecho de defensa.
   d) Cambio de las políticas de privacidad.
   e) Por Espionaje

2. **¿Conoce Ud. el tratamiento que realizan con sus datos íntimos las aplicaciones de Internet?**
   a) Beneficio económico con datos íntimos.
   b) Uso de información íntima.
   c) Control desigual de la información.
   d) Destino desconocido de la información.

3. **¿Cómo considera Ud. que son recogidos y almacenados sus datos Íntimos por las aplicaciones de Internet.**
   a) A través de perfiles de navegación online.
   b) Tráfico de datos.
   c) Registros obligatorios.
   d) A través de cuentas de internet.

4. ***¿De qué forma cree Ud. que se garantice el derecho a la intimidad en las aplicaciones de Internet?***
   a) Respetando la normativa nacional.
   b) Solicitando su consentimiento expreso.

5. ***¿Qué tipos de protección a la intimidad le gustaría que implementen las aplicaciones de Internet para sus usuarios?***
   a) Derecho al olvido
   b) Derecho de cancelación
   c) Notificar y retirar información
   d) Reparación de daños causados en Internet.
   e) Avisos de intromisiones.

Anexo 1 B
MATRIZ DE CONSISTENCIA DEL PROYECTO DE INVESTIGACIÓN

Problema de Investigación	Delimitación del Problema	Objetivos de la Investigación	Formulación de la Hipótesis	Método y Diseño de Investigación	Población y Muestra	Técnicas e Instrumentos
Problema Principal ¿Por qué las aplicaciones de internet afectan el derecho fundamental a la Intimidad de sus usuarios en el distrito de Paucarpata, Arequipa 2014 – 2015? **Problema Secundario** 1) ¿Cómo manejan las aplicaciones de Internet la intimidad de sus usuarios? 2) ¿De qué forma se vulnera la intimidad en las aplicaciones de Internet? 3) ¿Cómo proteger la intimidad de los usuarios en Internet?	**A. Social.** El presente trabajo abarca socialmente a todas aquellas personas o usuarios que puedan acceder a las aplicaciones de Internet. **B. Espacial.** La presente investigación sobre la vulneración al derecho fundamental de la intimidad se establece específicamente en la ciudad de Arequipa – Perú, en el distrito de Paucarpata. **C. Temporal.** Este trabajo investigativo, se desarrollará durante los años 2014 - 2015.	**Objetivo General** Analizar las aplicaciones de Internet que afectan el derecho fundamental a la intimidad de sus usuarios. **Objetivos Específicos** 1) Identificar el manejo que las aplicaciones de Internet dan la intimidad de sus usuarios. 2) Describir las formas de vulneración a la intimidad en las aplicaciones de Internet. 3) Determinar las formas de protección a la intimidad de los usuarios en Internet.	Es probable que la regulación de las aplicaciones de Internet a través de un marco normativo específico, garantice el derecho a la intimidad de los usuarios de internet. **Variables** **V. independiente:** Aplicaciones de Internet ***Indicadores*** 1) Vulneración **V. dependiente:** Derecho a la intimidad. ***Indicadores*** 1) Manejo de información 2) Formas de protección	**Método de investigación** Debido a que la investigación es de corte mixto, se adoptaron dos métodos. Tenemos al método de **Análisis e Interpretación Documental (Hermenéutico)** y seguido a ello tenemos al método de investigación **explicativo**. **Diseño de investigación** Se desarrollará uno corte analítico – explicativo, porque está basado en analizar y explicar las injerencias al derecho a la intimidad. Para ello se pondrá de manifiesto el empleo del ***análisis e interpretación documental,*** que se aplicará sobre fuentes de información, que determine el investigador de acuerdo con el problema de investigación. Seguidamente se detallará ***explicativamente*** mediante una encuesta que será aplicada a cada uno de los sujetos de investigación, seleccionados de manera aleatoria siendo en total 203 en contraste con la realidad.	**Población** Dado que será un trabajo de investigación mixta, se dispondrá en primer lugar un análisis e interpretación documental cualitativo de fuentes informativas, que determine el investigador de acuerdo con el problema de investigación, siendo los siguientes: 🏛 Constitución Política 🏛 Ley de protección de los datos personales 🏛 Doctrina 🏛 Marco Civil Brasileño 🏛 Políticas de privacidad de principales aplicaciones de Internet En segundo lugar cuantitativamente se tomará como población al distrito de Paucarpata obteniendo de ello con una confiabilidad del 50% un total de 203 personas de ambos sexos que serán la muestra.	**Técnicas** **Observación Documental** De acuerdo al diseño y problema de investigación, cualitativamente se ha utilizado la técnica de la observación documental, la cual consiste el ***acopio y análisis documental*** cuya selección, recopilación, análisis e interpretación de los datos se plasmará en un Cuadro de Análisis e Interpretación Documental. (C.A.I.D.). El objetivo principal de este instrumento es analizar y evaluar documentos y normas como referentes con las políticas de privacidad de las principales aplicaciones de Internet. **La Encuesta** Esta técnica corresponde a la parte cuantitativa del presente trabajo, dirigida a los usuarios de Internet para tener una visión más amplia sobre el problema y así contrastarlo con la realidad local para esbozar posibles soluciones.

Anexo 1 C
CUADRO DE ANÁLISIS E INTERPRETACIÓN DOCUMENTAL

Constitución Política del Perú	**Ley 29733 Ley de Protección de datos personales**	**Doctrina**	**Marco civil Brasileño**	**Facebook**	**Google**	**Microsoft**	
Intimidad Art.2 Inc. 6 A que los servicios informáticos, computarizados o no, públicos o privados, ***no suministren informaciones que afecten la intimidad*** personal y familiar. ***Art.2 Inc. 7*** Al honor y a la buena reputación, ***a la intimidad personal y familiar*** así como a la voz y a la imagen propias	**Datos personales**: Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados. **Datos sensibles**. Constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual. . Las disposiciones de esta Ley no son de aplicación a los siguientes datos personales: 1. A los contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.	*Este derecho define el poder de control de la persona sobre sus datos personales, sobre su uso y destino. El derecho a la intimidad personal y familiar y el derecho a la protección de datos,* ***aun siendo distintos tienen una base común: la dignidad de la persona humana y los derechos inviolables que le son inherentes*** **(Miranda Alcántara, 2003, pág. 7)**. Las aplicaciones de Internet al corresponden en la realidad a empresas que crean soportes virtuales para suplir una necesidad de los usuarios. **Vasquez R 2011** Las aplicaciones en internet son un conjunto de programas diseñados para la realización de una tarea concreta **Villaroig 2007.**	Marco sistemático que protege: ***Datos personales*** Inviolabilidad de la intimidad y vida privada Registros y secreto de comunicaciones ***Prohibición de Registros obligatorios*** Jurisdicción Que las empresas prestadoras de conexión como de aplicaciones respeten su normativa en función de sus usuarios ***Responsabilidad civil*** Donde no se responsabiliza al proveedor siempre que tome providencias para impedir la proliferación de contenidos ilegales o que una orden judicial lo ordene.	Presenta publicidad en función a las preferencias del usuario Sin un registro no es posible acceder a su servicio. Cuenta con canales de denuncia ante contenido inapropiado No informa sobre el uso y destino de los datos personales Sus políticas de privacidad cambian constantemente No discrimina entre datos personales y datos sensibles Cuenta con tecnología de cookies que rastrean datos de sus usuarios	**Gmail** Revisa el contenido de toda la información contenida en sus servidores Sin un registro no es posible acceder a su servicio. No informa sobre el uso y destino de los datos personales Sus políticas de privacidad cambian constantemente No discrimina entre datos personales y datos sensibles No cuenta con tecnología de cookies que rastrean datos de sus usuarios	**Outlook** Revisa el contenido de toda la información contenida en sus servidores Sin un registro no es posible acceder a su servicio. No informa sobre el uso y destino de los datos personales Sus políticas de privacidad cambian constantemente No discrimina entre datos personales y datos sensibles No cuenta con tecnología de cookies que rastrean datos de sus usuarios	Problema ¿Por qué las aplicaciones de internet afectan el derecho fundamental a la Intimidad de sus usuarios en el distrito de Paucarpata, Arequipa 2014 – 2015? Hipótesis Es probable que la regulación de las aplicaciones de Internet a través de un marco normativo específico, garantice el derecho a la intimidad de los usuarios de internet.

Anexo 1D

PROYECTO DE LEY Nº

"Decenio de las personas con discapacidad en el Perú"

"Año de la diversificación productiva y del fortalecimiento de la educación"

Sumilla: Proyecto de ley para la protección de la intimidad y los datos personales de los usuarios en las aplicaciones de internet usando diversas tecnologías de la comunicación

I. DATOS DEL AUTOR

El bachiller en Derecho y Ciencias Políticas de la Universidad Alas Peruanas que suscribe, Macedonio Enrique Santa Cruz Aco, en ejercicio de sus facultades ciudadanas, que le confiere el artículo 31 de la Constitución Política del Perú y el artículo 75 del reglamento del Congreso de la República, propone el siguiente Proyecto de Ley para la protección de la intimidad y los datos personales de los usuarios en las aplicaciones de internet usando diversas tecnologías de la comunicación.

LEY PARA LA PROTECCIÓN DE LA INTIMIDAD Y LOS DATOS PERSONALES DE LOS USUARIOS EN LAS APLICACIONES DE INTERNET USANDO DIVERSAS TECNOLOGÍAS DE LA COMUNICACIÓN

II. EXPOSICIÓN DE MOTIVOS

El presente proyecto promueve la participación integral del Estado, para legislar la problemática referida a la intimidad del usuario al hacer uso de las aplicaciones de Internet, abarcando desde acciones técnicas hasta el uso conjunto de instituciones educativas en pro de fomentar una conciencia sobre los riesgos de las aplicaciones de Internet y la forma adecuada de cómo proteger su derecho a la Intimidad y conexos.

El presente proyecto de ley versa sobre las aplicaciones de internet que vulneran el derecho fundamental a la Intimidad de sus usuarios y la debida protección de sus datos íntimos, el cual se basa en primer orden en el Art.2 Inc. 6 de nuestra Constitución Política del Perú, el cual prescribe "*A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar*". Ídem el Art. 2 Inc. 7 del mismo cuerpo legal que establece como derecho de la persona "*Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias*"; siguiendo con la línea de ideas, es deber del Estado promover el fortalecimiento y la aplicación de los preceptos constitucionales antes citados, es así que dentro de esta labor se debe buscar formas de impulsar el respeto de estas normas tanto para el ciudadano como para las diversas aplicaciones de Internet a las que accedemos, situando un equilibrio entre la promoción de la empresa en Internet con los derechos del ciudadano a la hora de acceder a esta red, todo ello en función al rol de protección e impulso de la tecnología hacia la sociedad, generando confianza y protegiendo la privacidad y los datos personales.

En concordancia con lo señalado, el derecho a la intimidad por ser un derecho personalísimo es un derecho inherente a la esencia de la persona, este derecho en el ámbito digital se manifiesta en ciertos datos que constituyen una extensión de nuestra personalidad, esto se refleja jurídicamente en una ley de reciente implementación conocida como "Ley de Protección de Datos Personales" que nace en función al Inc. 6 del Art. 2 de la Constitución para el ámbito digital, disponiendo "*La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.*" Lo cual hace referencia directa al derecho a la intimidad en el aspecto de dato personal.

De lo establecido anteriormente la ley no señala, hasta donde son sus alcances en lo referente a la red conocida como Internet, debido a que los citados referentes legales, no concluyen en una regulación específica referida a

la intimidad propiamente dicha en relación a las tan usadas e indispensables aplicaciones de Internet, pues, no existe una correspondencia legal de lo señalado y lo que sucede en la realidad, más aún cuando no existe un sistema jurídico específico y solo normas generales de orden constitucional u orientadas a proteger situaciones referentes al acceso a Internet, igual suerte corre la ley de protección de datos personales, que garantiza el Art.2 Inc. 6 de nuestra constitución, al está facultada para realizar una ponderación de derechos constitucionales ante un conflicto de estos, ni cuenta con vínculos con el Tribunal Constitucional que si puede hacerlo, del mismo modo, nuestro ordenamiento penal carece de flexibilidad en el sentido de establecer sus requisitos para configurar un ilícito, ni cuenta con formas de resarcir un daño al no poder establecer un sujeto imputable, de lo anterior se colige que la regulación y protección hacia el ciudadano es asistemática, aislada e inaccionable, en este sentido la norma no hace referencia a la protección y el ejercicio que se pueda hacer de los derechos sustanciales, en los casos de violación a los mismos, que pueda aplicarse a las actividades informáticas en Internet, pues no existe un marco que corresponda a la defensa de derechos tan singulares y propios.

Desarrollando la problemática en la realidad, se puede citar a Susana Navas Navarro, veamos:

> Cualquier actividad o consulta, que llevemos a cabo en internet, deja una huella o marca que permite nuestra identificación resultando casi inevitable que otros puedan acceder a esa información con un propósito (legítimo o ilegítimo) concreto. ***Esa huella personal permite la creación de perfiles online de los usuarios de internet, ya sea sobre la base de los datos que ellos mismos han suministrado acerca de sus gustos, preferencias, hábitos, información personal al consultar un sitio web*** (v. gr. Google, Amazon) o ya sea mediante su participación en una red social (v. gr. Facebook). Estos perfiles son creados normalmente, mediante un algoritmo, por terceros, a partir de la información recabada, tras la consulta de diferentes sitios web por los usuarios. **(Navas Navarro, 2015, pág. 1)**

Los perfiles así creados permiten a los prestadores de servicios o aplicaciones de Internet, presentar la denominada "publicidad online comportamental" es en este punto, donde el usuario de internet, siendo titular de su información personal o íntima, pierde prácticamente el control y destino sobre ella y es allí donde la intimidad de las acciones que se realizan en Internet a través de aplicaciones se ve vulnerada, de igual forma no debe olvidarse, que al hacer uso de estas tecnologías aceptamos un acuerdo, el mismo que al analizarse rigurosamente y legalmente trae consigo el empleo de términos confusos, ambiguos, haciéndose remisiones entre diferentes políticas como, por ejemplo, de la política de privacidad general a la política de cookies o viceversa, se fragmenta deliberadamente la información para evitar que el usuario tenga conocimiento cabal de sus derechos y obligaciones así como de los derechos y obligaciones del titular del sitio web o aplicación, es así que desde el punto de vista jurídico, una forma de intentar frenar esta asimetría, en cuanto al control de la información personal del usuario de internet, se encuentra en regular los puntos citados mediante un marco legal sistemático.

A. Realidad online en el Perú.

La cantidad de usuarios que navega en Internet se ha visto incrementado tanto por la forma de acceder que va desde un celular hasta una Tablet, como en el tiempo de consumo, es por ello que se dice que en nuestro país hay una mayor penetración de Internet y con ello un incremento en el tiempo que se usa la red, "*pero aún somos pura interacción social, según ComScore Perú*" **(Mendoza Riofrío, 2014)**

Según el diario El Comercio, "se triplicó la cantidad de conexiones a Internet vía celular (pasamos de 5% a 17% de penetración en el último año) y en Lima 6 de cada 10 hogares tienen Internet fijo" **(Mendoza Riofrío, 2014)**.

De lo expuesto, la preferencia en el consumo de la red, revela que ocupamos mucho tiempo en las redes sociales, veamos:

> "El último estudio publicado por ComScore Perú no deja lugar a las dudas: los peruanos somos facebookeros y pasamos mucho más tiempo que el promedio regional entretenidos viendo quién publicó qué. Las cifras no mienten: Perú concentra 5,8 millones de usuarios online, de los cuales 5,1 millones tienen Facebook. Además, como si no fuera

suficiente, el 97% del tiempo que nos conectamos (18,2 horas en promedio al mes) es para visitar a la chismosita blanquiazul. **(Mendoza Riofrío, 2014)**

Esta información esta graficada en la Figura 1.

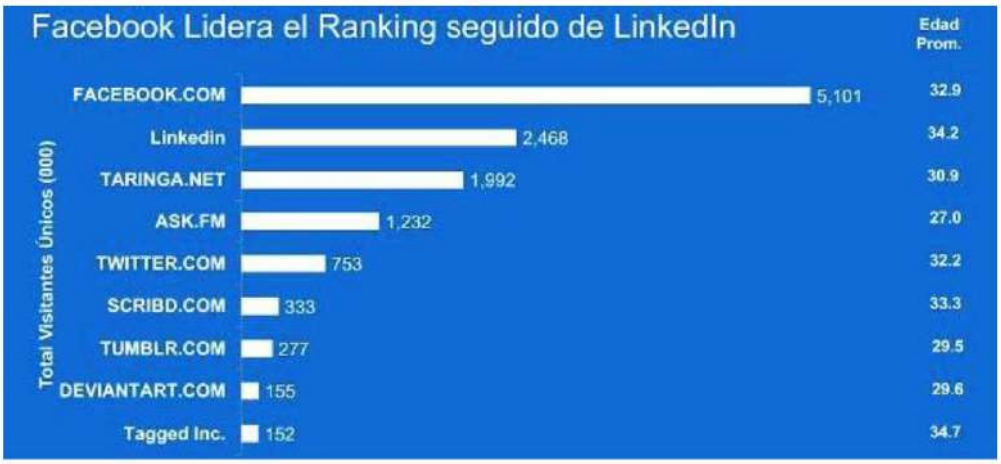


Fig. 1 Ranking de las principales redes sociales en Perú Fuente: Diario El comercio

De acuerdo a las estadísticas proporcionadas por ComScore al diario El Comercio, la población peruana cuenta con una participación bastante representativa en Internet, tal como señala el artículo presentado por **(Mendoza Riofrío, 2014),** "*pasamos más horas en Internet que los colombianos, estamos por encima del promedio mundial en horas por visitante a las redes sociales y crecimos 17% el número de usuarios de la red mientras que Chile solo creció 9%*".

En cuanto al análisis de esta realidad el mismo artículo señala que no es que navegamos en función a las redes sociales, veamos "LinkedIn, la red social laboral por excelencia, tiene la mitad de visitantes que Facebook, Twitter apenas y paso los 700 mil enlistados, el BCP (el banco más visitado) bordea los 666 mil visitantes únicos y Lan Perú con las justas supera los 378 mil (15% menos que el año pasado). Y eso que hasta ahí solo hemos hablado de las actividades más frecuentes en Internet - operaciones bancarias y compra de pasajes - luego de la interacción con familia y amigos" **(Mendoza Riofrío, 2014)**.

Estamos despertando al mundo online, sí. Hemos mejorado el nivel de acceso al Internet y sus beneficios en la vida prácticas, sí. Cada

> vez tenemos más smartphone que acceden a un plan de datos, sí. Pero nos falta mucho para sacarle el verdadero potencial productivo, económico, comercial y práctico que ofrece la red de redes. **Progreso va más allá de estar enlazados a las redes sociales**, estamos seguros, y hacia ahí es adonde, esperamos, nos encaminemos este año los cibernautas. Facebook es muy bonito - me encanta, lo admito - pero no lo es todo en estos lares.
>
> **(Mendoza Riofrío, 2014)**

Es de conocimiento real y documental que uno de los lugares donde se vislumbra en mayor proporción vulneraciones a la intimidad son las redes sociales y las aplicaciones comunicativas de internet, dentro de lo señalado las estadísticas expresan que Facebook es el líder en cuanto a redes sociales se refiere, para el tiempo en que se desarrolla el presente trabajo, siendo el más concurrido por la audiencia peruana, es así, que dentro de las aplicaciones de internet es la que debe recibir un tratamiento diferenciado, al ser la de mayor número de peruanos usuarios.

III. PROPUESTA DE INCLUSIÓN LEGISLATIVA

Se propone agregar una norma que complemente el corpus legal vigente, en los aspectos que refieren a la protección de la intimidad y los datos personales de los usuarios en las aplicaciones de internet, usando diversas tecnologías de la comunicación.

IV. EFECTOS DE LA VIGENCIA DE LA NORMA

En la eventualidad de que se apruebe el presente proyecto de ley, se brindará un sustento real dirigido a proteger al usuario mientras utiliza Internet, esto generará un clima de seguridad jurídica y un estado de derecho democrático, para brindar una protección real del derecho a la intimidad y la debida protección de datos personales de toda persona que utiliza las nuevas tecnologías de la comunicación, fortaleciendo lo protegido por nuestra constitución política.

V. ANÁLISIS DEL COSTO BENEFICIO

La señalada propuesta legislativa, conlleva un trabajo conjunto de los diversos organismos del Estado, en promoción de la intimidad de las personas denominadas usuarios de Internet, esto no generará un costo significativo al Estado, sino, un trabajo logístico más complejo, pues el Ministerio de Justicia y Derechos Humanos se encarga de defender elementalmente los derechos de las personas en función de sus datos personales, sin considerar las diversas aplicaciones de Internet que manipulan o recopilan información intima de sus usuarios.

VI. FÓRMULA LEGAL

CAPÍTULO I
DISPOSICIONES PRELIMINARES

Art. 1 Esta Ley establece los principios, garantías, derechos y obligaciones para el uso de Internet, específicamente de las aplicaciones que mayor impacto social tengan en Perú y determina las pautas para la actuación y defensa de los derechos referidos a la intimidad y conexos, de los usuarios que navegan usando aplicaciones de Internet.

Art. 2 La presente ley se sustenta en el uso razonable, equilibrado y neutral de Internet y las aplicaciones que recopilan, usan, comparten entre otros datos de los usuarios en relación a su derecho a la intimidad y conexos, ello en base al respeto de las garantías fundamentales que goza toda persona, pilar básico de nuestra legislación, es así que reconoce los siguientes principios en la red:

I - el reconocimiento de la presencia mundial de la red;

II - los derechos humanos, el desarrollo de la personalidad y de la ciudadanía en los medios digitales;

III - la pluralidad y la diversidad;

IV- la apertura y la participación;

V- la libre empresa, la libre competencia y protección del consumidor; y la finalidad social de la red.

Art. 3 El uso de Internet debe observar los siguientes principios:

I. El reconocimiento del acceso a Internet como un Derecho humano.
II. El reconocimiento de la dignidad de la persona como garantía en la red
III. Garantía de la libertad de expresión, la comunicación y la manifestación del pensamiento, según la Constitución;
IV. Protección de la intimidad, privacidad y datos personales, en la forma de ley;
V. Garantía de la estabilidad jurídica y el derecho a la defensa.
VI. Preservación de la garantía de neutralidad de la red;
VII. Observancia de la garantía de autodeterminación informativa
VIII. Respeto al principio de consentimiento informado en la red
IX. Defensa de la estabilidad, seguridad y funcionalidad de la red, a través de medios técnicos, compatibles con patrones internacionales y el estímulo al uso de buenas prácticas;
X. Responsabilidad de las partes de acuerdo con sus actividades, en los términos establecidos por ley;
XI. Conservar la naturaleza participativa y colectiva de la red
XII. La protección de la personalidad e intimidad virtual es regla general.
XIII. El incentivo de implementación y aplicación del derecho al olvido
XIV. El equilibrio en el derecho a la defensa entre los usuarios y las aplicaciones de Internet
XV. El principio de representación del estado ante litigios
XVI. La libertad de empresa y los modelos de negocio promovidos vía internet, siempre que no interfieran con otros principios establecidos en esta ley.

Los principios expresados en esta ley, no excluyen otros previstos en el ordenamiento jurídico nacional relacionados con el tema, o los tratados internacionales en los que participe nuestro país, siempre que tenga en consideración la dignidad de la persona ante todo.

Art. 4 El presente cuerpo legal, busca establecer los siguientes objetivos:

I. Defender el derecho de acceso a Internet en la sociedad

II. Impulsar el acceso a la información, al conocimiento y a la participación en la vida cultural en la conducción de asuntos públicos.
III. Promover la libre iniciativa y libre competencia
IV. Fomentar la innovación y promover una difusión amplia de nuevas tecnologías y modelos de uso y acceso; y
V. Promover la adherencia a los padrones tecnológicos abiertos que permitan la comunicación, accesibilidad y la interoperabilidad entre aplicaciones y bases de datos a partir del uso de estándares abiertos.
VI. Garantizar la intimidad, privacidad y datos personales, para mejorar la confianza de los usuarios y generar seguridad.

DEFINICIONES

Art. 5 A efectos de esta ley se entiende:

A. Internet: El sistema constituido por un conjunto de protocolos de software, estructurados a escala mundial para el uso público y sin restricciones, con la finalidad de posibilitar la comunicación de datos entre terminales por medio de diferentes redes;
B. Terminal: una computadora o cualquier dispositivo que se conecte a Internet;
C. Administrador de sistemas autónomo: persona física o jurídica que administra bloques de direcciones IP (Internet Protocol) específicas y el respectivo sistema autónomo de enrutamiento, debidamente registrada en el ente nacional responsable del registro y distribución de direcciones IP geográficamente relacionadas con el país;
D. Dirección IP: código atribuido a un terminal de una red para permitir su identificación, definido según parámetros internacionales;
E. Conexión a Internet: habilitación de un terminal para envío o recepción de paquetes de datos por Internet, mediante la atribución o autenticación de una dirección IP;
F. Registro de conexión: conjunto de informaciones referentes a datos y hora de inicio y término de una conexión a Internet, su duración e la dirección IP utilizada por el terminal para el envío y recepción de paquetes de datos;

G. Aplicaciones de Internet: conjunto de funcionalidades que pueden ser usadas por medio de un terminal conectado a Internet; y
H. Registros de acceso a aplicaciones de Internet: conjunto de informaciones referentes a datos y hora de uso de una determinada aplicación de Internet a partir de una determinada dirección IP.

Art. 6 En la interpretación de esta Ley se tendrán en cuenta, más allá de los fundamentos, principios y objetivos, la naturaleza de Internet, sus usos y costumbres particulares, así como, su importancia para la promoción del desarrollo humano, económico, social y cultural.

CAPÍTULO II
DE LOS DERECHOS Y GARANTÍAS DE LOS USUARIOS

Art. 7 El acceso a internet es esencial para el ejercicio de la ciudadanía y el usuario están garantizados los siguientes derechos:

I. La inviolabilidad de la intimidad y de la vida privada, asegurando el derecho a su protección y a la indemnización por el daño material o moral resultante de su violación;
II. La inviolabilidad del flujo y secreto de las comunicaciones por Internet, salvo por orden judicial, de acuerdo con la ley;
III. La inviolabilidad y el secreto de sus comunicaciones privadas almacenadas, salvo por orden judicial;
IV. La no suspensión de la conexión a Internet, salvo deuda contraída directamente por su utilización;
V. El mantenimiento de la calidad de la conexión a Internet contratada;
VI. Las informaciones claras y completas en los contratos de prestación de servicios, detallando en clausula separada, el régimen de protección de datos, los registros de conexión y los registros de acceso a las aplicaciones en Internet, así como de las prácticas de gestión de la red que puedan afectar a su calidad; y
VII. La imposibilidad de suministrar a terceros datos personales, incluyendo registros de conexión y acceso a aplicaciones en Internet, salvo

mediante consentimiento libre, expreso e informado o en aquellas circunstancias establecidas por la ley;

VIII. La información clara y completa sobre el recojo, uso, almacenamiento, tratamiento y protección de datos personales, que sólo podrán ser utilizados para finalidades que:

a) Justifiquen su recolección;

b) No estén prohibidas por ley; y

c) Queden especificadas en clausula separada en los contratos de prestación de servicios o en los términos de uso de las aplicaciones de Internet.

IX. El consentimiento expreso e informado sobre el recojo, uso, almacenamiento y tratamiento de datos personales, que deberá presentarse en clausula separada y de forma destacada de las demás cláusulas contractuales;

X. El borrado definitivo de los datos personales que se hayan proporcionado a determinada aplicación de Internet, a solicitud del usuario, al término de la relación entre las partes, salvo en los casos de custodia obligatoria de registros previstos en esta ley;

XI. La publicación y claridad de las eventuales políticas de uso por parte de los proveedores de conexión a Internet y de las aplicaciones de Internet;

XII. La accesibilidad, teniendo en cuenta las características físico-motoras, perceptivas, sensoriales, intelectuales y mentales del usuario, en los términos definidos por la ley;

XIII. La aplicación de las normas de protección y defensa del consumidor en las relaciones de consumo realizadas en Internet y las diversas aplicaciones; y

XIV. Cada aplicación de Internet implementará un libro de reclamaciones virtual que será transferido mensualmente a la entidad correspondiente de velar por los derechos del usuario como consumidor.

Art. 8 La garantía del derecho a la intimidad, privacidad y a la libertad de expresión en las comunicaciones es condición para el pleno ejercicio del derecho de acceso a Internet.

La presente ley vela por el cumplimiento del consentimiento, en tal sentido, debe cumplir con los siguientes principios y criterios para considerar la validez de la aceptación en las aplicaciones de Internet:

I. Descripción – resumen de los términos relacionados a la intimidad en cuanto a los objetivos o fines de recojo de información así como el destino que tendrán luego de recogidos.

II. Aviso oportuno sobre qué datos serán recogidos y cuál será el destino de los mismos.

III. Riesgos que supone una eventual aceptación de las mencionadas condiciones.

IV. Beneficios que resultarían de aceptar las condiciones de las políticas de privacidad en términos del derecho a la intimidad.

V. Alternativas de no aceptarse las cambiantes condiciones de políticas de privacidad.

VI. Comunicación – posibilidades de la información, es decir sugerir cambios con un tiempo razonable para tomar una decisión adecuada a las posibilidades sugeridas.

VII. Libertad para escoger, se entiende que al cambiar el sentido de las políticas de privacidad se cambian los términos contractuales de uso de un determinado servicio, ello debe darse en igualdad de condiciones para negociar y plantear alternativas beneficiosas a los usuarios en respeto de sus derechos en consonancia con los derechos de la persona jurídica que proporciona determinada aplicación en Internet.

CAPÍTULO III

DE LA PROVISIÓN DE CONEXIÓN Y DE APLICACIONES DE INTERNET

De la Neutralidad de la Red

Art. 9 El responsable de la transmisión, conmutación o ruteo tiene el deber de tratar de igual forma cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación.

Inc. 1 La discriminación o degradación del tráfico será reglamentada en los términos de las atribuciones privativas del Presidente de la República previstas en el inciso IV del artículo 84 de la Constitución Federal, para la

ejecución fiel de esta Ley, consultando con el Comité Gestor de Internet y la Agencia Nacional de Telecomunicaciones y solamente podrá ser resultado de:

1. requisitos técnicos indispensables para la prestación adecuada de los servicios y aplicaciones; y
2. priorización de los servicios de emergencia.

Inc. 2 En el caso de discriminación o degradación del tráfico prevista en el § 1°, el responsable mencionado en el artículo debe:

1. abstenerse de causar daño a los usuarios, de acuerdo con lo dispuesto en el Art. 927 del Código Civil;
2. actuar con proporcionalidad, transparencia e igualdad ante la ley;
3. informar previamente de modo transparente, claro y suficientemente descriptivo a sus usuarios sobre las prácticas de gestión y reducción del tráfico adoptadas, inclusive las relacionadas con la seguridad de la red; y
4. ofrecer servicios en condiciones comerciales no discriminatorias y abstenerse de practicar conductas anticompetitivas.

Inc. 3 En el suministro de la conexión a Internet, de pago o gratuita, así como en la transmisión, conmutación o enrutamiento, está prohibido bloquear, monitorizar, filtrar o analizar el contenido de los paquetes de datos, respetando lo dispuesto en este artículo.

El tráfico de datos

Art. 10 El responsable por la transmisión, conmutación o enrutamiento está obligado a tratar de forma igualitaria cualquiera paquete de datos, contenido, servicio, terminal o aplicativo, encontrándose prohibido establecer cualquier tipo de discriminación o degradación del tráfico que no se encuentre vinculada con los requisitos técnicos destinados a preservar la calidad contractual del servicio.

Protección de registros, datos personales y comunicaciones privadas

Art. 11. La custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet de que trata esta Ley, así como de los datos personales y del contenido de las comunicaciones privadas, deben atender a la preservación de la intimidad, vida privada, honra e imagen de las partes directa o indirectamente envueltas.

Inc. 1 El proveedor responsable de la custodia solamente será obligado a entregar los registros mencionados en el artículo, de forma autónoma o asociados a datos personales u otras informaciones que puedan contribuir a la identificación del usuario o del terminal, mediante orden judicial, tal como queda dispuesto en la Sección IV de este Capítulo, respetando lo dispuesto en el artículo 7.

Inc. 2 El contenido de las comunicaciones privadas solamente podrá ser entregado mediante orden judicial, en los casos y forma que establece la ley, respetando lo dispuesto en los parágrafos II y III del artículo 7.

Inc. 3 Lo dispuesto en este artículo no impide el acceso, por parte de las autoridades administrativas que detenten competencia legal para su solicitud, a los datos de registro que contengan información personal, filiación y dirección, de acuerdo con la ley.

Inc. 4 Las medidas y procedimientos de seguridad y secreto deben ser informados por el responsable de la provisión de servicios de forma clara y atenerse a patrones definidos en reglamento, respetando su derecho de confidencialidad en lo que respecta a secretos empresariales.

Art. 12. En cualquier operación de recolección, almacenamiento, protección o tratamiento de registros, datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de Internet en las que por lo menos uno de estos actos ocurra en territorio nacional, deberá ser obligatoriamente respetada la legislación nacional, los derechos a la privacidad y a la protección de los datos personales y al secreto de las comunicaciones privadas y de los registros.

Inc. 1 Lo dispuesto en el artículo se aplica a los datos recolectados en territorio nacional y al contenido de las comunicaciones en las cuales por lo menos uno de los dos está localizado en territorio peruano.

Inc. 2 Lo dispuesto en este artículo se aplica también, aunque las actividades sean llevadas a cabo por personas jurídicas domiciliadas en el exterior, siempre que oferten servicios al público peruano o que al menos una integrante del mismo grupo económico posea un establecimiento en Perú.

Inc. 3 Los proveedores de conexión y de aplicaciones de internet deberán presentar, en línea con la reglamentación, información que permita la verificación del cumplimiento de la legislación peruana en lo referente a la recolección, protección, almacenamiento o tratamiento de datos, así como en lo que respecta a la privacidad y al secreto de las comunicaciones.

Inc. 4 Un decreto reglamentará el procedimiento de determinación de infracciones a lo dispuesto en este artículo.

Art. 13. Sin perjuicio de las demás sanciones civiles, penales o administrativas, las infracciones a las normas previstas en los artículos 11 y 12 quedan sujetas, según el caso, a las siguientes sanciones, aplicadas de forma individual o acumulativa:

1. Advertencia, con indicación de plazo para la adopción de medidas correctivas;
2. Multa de hasta el quince por ciento de lo facturado por el grupo económico en Perú en su último ejercicio, excluidos los impuestos, considerando la condición económica del infractor y el principio de proporcionalidad entre la gravedad de la falta y la gravedad de la sanción;
3. Suspensión temporal de las actividades que involucren los actos previstos en el artículo 12; o
4. Prohibición de ejercicio de las actividades que involucran los actos previstos en el artículo 12.
5. Cuando se trate de una empresa extranjera, esta responderá solidariamente al pago de la multa de que trata este artículo su filial, sucursal, oficina o establecimiento situado en el país.

De la Custodia de Registros de Conexión

Art. 14. En la provisión de conectividad a Internet, cabe al administrador del sistema autónomo respectivo le deber de mantener los registros de

conexión, bajo secreto, en un ambiente controlado y seguro, por el plazo máximo de seis (6) meses, en los términos de la reglamentación administrativa posterior.

Inc. 1 La responsabilidad de mantener los registros de conexión no pueden ser transferida a terceros.

Inc. 2 La autoridad especializada, administrativa o el Ministerio Público podrá requerir cautelarmente que los registros sean guardados durante un plazo superior al previsto en este artículo.

Inc. 3 En los supuestos del Inc. 2, la autoridad solicitante tendrá el plazo de sesenta días, contados a partir de la solicitud, para ingresar, con el pedido de autorización judicial, a los registros previstos en este artículo.

Inc. 4 El proveedor responsable de la custodia de los registros deberá mantener el secreto en relación a la solicitud prevista en Inc. 2, que perderá su eficacia en caso de que el pedido de autorización judicial no sea aceptada o no haya sido ejecutada en el plazo previsto en Inc. 3.

Inc. 5 En cualquier caso, la disposición al requirente de los registros de los que trata este artículo, deberá ser precedida de una autorización judicial, conforme a lo dispuesto en la Sección IV de este capítulo.

Inc. 6 En la aplicación de sanciones por el incumplimiento de lo dispuesto en este artículo, serán considerados la naturaleza, la gravedad de la infracción y los daños resultantes de ella, eventual beneficio para el infractor, las circunstancias agravantes, los antecedentes del infractor y la reincidencia.

De la Custodia de Registros de Acceso a Aplicaciones de Internet en la Provisión de Conexión

Art. 15. En la provisión de conexión, onerosa o gratuita, está prohibido almacenar registros de acceso a aplicaciones de Internet.

De la Custodia de Registros de Acceso a Aplicaciones de Internet en la Provisión de Aplicaciones de Internet

Art 16. El proveedor de aplicaciones de Internet constituido en forma de persona jurídica, que ejerza esa actividad en forma organizada, profesionalmente y con fines económicos, dentro y fuera del país, deberá mantener los respectivos registros de acceso a aplicaciones de internet, en

secreto, en ambiente controlado y de seguridad, por un plazo de seis meses, en los términos del reglamento.

Inc. 1 Una orden judicial podrá obligar, por tiempo determinado, a los proveedores de aplicaciones de Internet, que no estén sujetos a lo dispuesto en el artículo a guardar registros de acceso a aplicaciones de Internet, siendo que se tratan de registros relativos a hechos específicos en un tiempo determinado.

Inc. 2 La autoridad especializada, administrativa o el Ministerio Público podrán solicitar cautelarmente a cualquier proveedor de aplicaciones de Internet que los registros de acceso a aplicaciones de Internet sean guardados, inclusive por plazo superior al previsto en el artículo, observando lo dispuesto en Inc. 3 y 4 del Art. 14.

Inc. 3 En cualquier caso, la disposición al requirente, de los registros de los que trata este artículo, deberá ser precedida de autorización judicial.

Inc. 4 En la aplicación de sanciones por el incumplimiento de lo dispuesto en este artículo, serán considerados la naturaleza y gravedad de la infracción, los daños resultantes de ella, el eventual beneficio para el infractor, las circunstancias agravantes, los antecedentes del infractor y la reincidencia.

Art. 17. En la provisión de conexión, onerosa o gratuita, está prohibida la custodia de:

1. los registros de acceso a otras aplicaciones de Internet sin que el titular de los datos haya consentido expresa, en clausula separada y previamente, respetando lo dispuesto en el art. 7; y
2. datos personales que sean excesivos en relación a la finalidad para la cual fue dado el consentimiento por su titular.

Art. 18. Excepto en los casos previstos en esta Ley, la opción de no guardar los registros de acceso a aplicaciones de Internet no implica responsabilidad sobre los datos que surgieran del uso de esos servicios por terceros.

De la Responsabilidad por Daños que Surgieran del Contenido Generado por Terceros

Art. 19. El proveedor de conexión a internet no será responsabilizado civilmente por daños surgidos por contenido generado por terceros.

Art. 20. Con el objetivo de asegurar la libertad de expresión e impedir la censura, el proveedor de aplicaciones de Internet solamente podrá ser responsabilizado por daños que surjan del contenido generado por terceros si, después de una orden judicial específica, o algún trámite administrativo no toma las previsiones para, en el ámbito de los límites técnicos de su servicio y dentro del plazo asignado, hace disponible o bloquea el contenido especificado como dañoso, exceptuando las disposiciones legales que se opongan.

Inc. 1 La orden judicial de que trata este artículo deberá contener, bajo pena de nulidad, identificación clara y específica del contenido especificado como dañoso, que permita la localización inequívoca del material.

Inc. 2 El procedimiento administrativo seguido ante la autoridad nacional de datos personales o ante el mismo proveedor de la aplicación de Internet, tendrá validez siempre y cuando no se siga un procedimiento ante la autoridad nacional de datos personales o ante el poder judicial en ese orden de preeminencia, absteniéndose de resolver si alguno de ellos tiene conocimiento, caso contrario deberá constatar, bajo pena de nulidad, la identidad del reclamante, la caracterización clara y específica del contenido especificado como dañoso, que permita la localización inequívoca del material.

Inc. 3 La aplicación de lo dispuesto en este artículo para infracciones a derechos de autor y a derechos conexos depende de la previsión legal específica, que deberá respetar la libertad de expresión y las demás garantías previstas.

Inc. 4 Las causas judiciales que traten sobre el resarcimiento por daños surgidos de contenidos disponibilizados en Internet relacionados a la honra, la reputación y a derechos de personalidad así como sobre la indisponibilización de esos contenidos por proveedores de aplicaciones de internet podrán ser presentadas mediante los juzgados especiales.

Inc. 5 El juez, incluso en el procedimiento previsto en Inc. 4, podrá anticipar, total o parcialmente, los efectos de la tutela pretendida en el pedido inicial, existiendo la prueba inequívoca del hecho y considerando el interés de la

colectividad en la disponibilización del contenido en Internet, estando presentes requisitos de verosimilitud de la alegación del autor o persona y temor fundado de daño irreparable o de difícil reparación.

Art. 21. Siempre que tenga informaciones de contacto del usuario directamente responsable por el contenido al que se refiere el Art. 20, corresponderá al proveedor de aplicaciones de Internet comunicarle los motivos e informaciones relativos a la indisponibilización de contenido, con informaciones que permitan la contradicción y amplia defensa en juicio, salvo expresa previsión legal o salvo expresa determinación judicial fundamentada en contra.

Inc.1. Cuando sea solicitado por el usuario que hizo disponible el contenido que ha sido hecho indisponible, el proveedor de aplicaciones de Internet que ejerza esa actividad de forma organizada, profesionalmente y con fines económicos, sustituirá el contenido indisponible, por la motivación o por la orden judicial que fundamenta la indisponibilización.

Art. 22. El proveedor de aplicaciones de internet que disponibilice contenido generado por terceros será responsabilizado subsidiariamente por la violación de la intimidad resultado de la divulgación, sin autorización de sus participantes, de imágenes, videos u otros materiales que contengan escenas de desnudos o de actos sexuales de carácter privado cuando, posterior al recibimiento de la notificación por el participante o su representante legal, deja de promover, de forma diligente, en el ámbito y en los límites técnicos de su servicio, la indisponibilización de ese contenido.

Inc. 1 La notificación prevista en el artículo deberá contener, bajo pena de nulidad, elementos que permitan la identificación específica del material apuntado como violador de la intimidad del participante y la verificación de la legitimidad para presentación del pedido.

De la Solicitud Judicial de Registros

Art. 23. La parte interesada podrá, con el propósito de formar conjunto probatorio en proceso judicial civil o penal, en carácter incidental o autónomo, requerir al juez que ordene al responsable por la guarda u otorgamiento de registros de conexión o de registros de acceso a aplicaciones de Internet.

Inc. 1 Sin perjuicio de los demás requisitos legales, el requerimiento deberá contener, bajo pena de inadmisibilidad:

1. fundados indicios del acontecimiento del ilícito;
2. justificación motivada de la utilidad de los registros solicitados para fines de investigación o instrucción probatoria; y
3. período al cual se refieren los registros.

Art. 24. Cabe al juez tomar las providencias necesarias la garantía del sigilo de las informaciones recibidas y la preservación de la intimidad, vida privada, honra e imagen del usuario, pudiendo determinar secreto de justicia, inclusive en cuanto a los pedidos de guarda de registro.

CAPÍTULO IV:
PRÁCTICA DEL PODER PÚBLICO

Art. 25. El presente documento, constituye una directriz para el accionar jurídico en todas las provincias del país, en concordancia con el desarrollo y promoción del acceso a Internet garantizado y neutral para todos los ciudadanos, en tal sentido:

1. se establecerán mecanismos de administración multiparticipativa, transparente, colaborativa y democrática, con participación del gobierno, el sector empresarial, la sociedad civil y la comunidad académica;
2. habrá promoción de la racionalización de la gestión, la expansión y el uso de Internet, con la participación de los principales Stakeholders de nuestro país;
3. existirá promoción de la racionalización y la interoperabilidad tecnológica de los servicios de gobierno electrónico, entre los diferentes Poderes y niveles de organismos gubernamentales, para permitir el intercambio de información y la rapidez de los procedimientos;

4. se implementará la interoperabilidad entre los diversos sistemas y terminales, incluso entre los diferentes sectores de la sociedad;
5. se adoptará preferencialmente las tecnologías, estándares y formatos abiertos y libres;
6. la publicidad y difusión de los datos y la información pública, será abierta y estructurada;
7. se optimizará las redes de infraestructura y se fomentara la creación de centros de almacenamiento, gestión y difusión de datos en el país, promoviendo la excelencia técnica, la innovación y la difusión de las aplicaciones de Internet, sin perjuicio de la apertura, la neutralidad y la naturaleza participativa;
8. habrá desarrollo de acciones y programas de capacitación para el uso de Internet, tanto para la sociedad civil como para los diferentes niveles educativos incluyendo la educación superior pública y privada;
9. se buscará la promoción de la cultura y la ciudadanía; y
10. habrá prestación de servicios públicos de atención al ciudadano de forma integral, eficiente, simple y por múltiples vías de acceso, inclusive a distancia.

Art. 26. Los aplicativos o aplicaciones de Internet de los entes del Poder Público deben procurar:

1. compatibilidad de los servicios de gobierno electrónico con diferentes terminales, sistemas operativos y aplicaciones de acceso;
2. accesibilidad a todos los interesados, independientemente de sus capacidades físico-motoras, perceptivas, sensoriales, intelectuales, mentales, culturales y sociales, salvaguardando los aspectos referidos a los derechos de personalidad y restricciones administrativas y legales;
3. compatibilidad tanto con la lectura humana como con el tratamiento automatizado de la información;

4. ser de preferencia de estándares, formatos libres o abiertos
5. facilidad de uso de los servicios de gobierno electrónico; y
6. promover la participación social en las políticas públicas.

Art. 27. El cumplimiento de la obligación constitucional del Estado en la provisión de la educación, en todos los niveles de enseñanza, incluida la capacitación, integrada con las otras prácticas educativas, para un uso seguro, consciente y responsable de Internet, como herramienta para el ejercicio de la ciudadanía, la promoción de la cultura y el desarrollo tecnológico.

Art. 28. Las iniciativas públicas que promueven la cultura digital y el uso de Internet como herramienta social deben:

1. Buscar la inclusión digital;
2. Reducir las desigualdades, sobre todo entre las diferentes regiones del País, en el acceso a tecnologías de la información y comunicación así como su uso; y
3. Promover la producción y difusión de contenido nacional.
4. Resaltar los valores patrios y el amor a la nación.

Art. 29. El Estado debe, anualmente, formular y fomentar estudios, así como fijar metas, estrategias, planes y programas relacionados al uso y desarrollo de Internet en el País, así como, la debida actualización de acciones y políticas de desarrollo sobre la red, adiciones normativas al presente cuerpo normativo y nuevas formas de protección al ciudadano acorde a los avances tecnológicos, a cargo de las autoridades competentes en una mesa de cooperación.

CAPÍTULO V:
DISPOSICIONES FINALES

Art. 30. El usuario tendrá libre elección en el uso de software en su terminal para facilitar el control parental de contenidos, según considere impropio para sus hijos menores, siempre y cuando cumplan con los principios de esta Ley y los demás cuerpos normativos.

Inc. 1. Corresponde al Gobierno, en conjunto con los proveedores de conexión y aplicaciones de Internet y la sociedad civil, promover la educación y proporcionar información sobre el uso de los programas de ordenador definidos anteriormente, así como para la definición de buenas prácticas para la inclusión digital de niños y adolescentes.

Art. 31. La defensa de los intereses y derechos establecidos en esta ley podrá ser ejercida individual, colectivamente, a través del defensor del pueblo, ministerio público u otros conforme a lo dispuesto por esta ley o en concordancia con la normativa vigente.

Art. 32. Las decisiones que, sobre la modificación, adopción o negociación sobre acuerdos comerciales u otros que se relacionen con las TICs, intimidad, protección de datos y otros que sean conexos a los derechos de personalidad y otros protegidos por la constitución, serán sometidos a referéndum, para negociar y hacer participar a la sociedad y otros organismos en las decisiones que se tomarán a posterior, conforme lo establece la constitución y en concordancia con el ordenamiento normativo vigente.

Art. 33. En los casos de geolocalización, o investigaciones en los que se haga uso y tratamiento de datos personales y conexos a la persona, su personalidad y dignidad, concluida la investigación o no, se comunicará al usuario investigado sobre la naturaleza de la investigación y el delito que se persigue para que se haga de su conocimiento dichos actos, así como para hacer sus descargos o ejercer sus respectivos derechos, si considerase arbitrarias dichas investigaciones, el periodo de reserva de los concesionarios de los servicios públicos de telecomunicaciones y otras entidades análogas, guardarán un periodo de reserva de 30 días hábiles o más, a solicitud del juez de forma fundamentada y bajo responsabilidad del mismo, luego del cual, se comunicará al respectivo usuario mediante llamadas u otro medio, lo siguiente: el tenor de la investigación, el periodo de tiempo que fue investigado y el delito del que se le está acusando, esta disposición podrá ampliarse por otros 30 días más, a solicitud del ministerio público con la anuente del juez que conoce del proceso, bajo responsabilidad del mismo, así mismo, los concesionarios de los

servicios públicos de telecomunicaciones y otras entidades análogas que brindaron datos a la investigación, cursarán un oficio de conocimiento, de la solicitud de datos de localización y geolocalización, a la oficina de control de la magistratura para que verifique el exacto y real cumplimiento de las normas en razón de velar por el respeto de la intimidad de la persona y sus derechos, ante un caso de violación, vulneración o injerencia de que este haciendo el aparato judicial.

Art 34. Establézcanse convenios de colaboración entre los principales buscadores, redes sociales y otras aplicaciones de internet que tengan alta relevancia social en función a la intensidad de uso de la población, en materia de privacidad, y otros que correspondan a los derechos humanos de la personalidad, recogidos y protegidos por la constitución política del Perú.

Art 35. En caso de no acatar las disposiciones señaladas en art. Anterior, se aplicará lo dispuesto por el art. 13, así como de las demás sanciones pertinentes, y se tomará en cuenta y se tratará de hacer convenios con los países donde se ubiquen los servidores de las mencionadas aplicaciones de Internet que se nieguen a acatar nuestra legislación o convenio de colaboración.

Art. 36. Hasta la entrada en vigencia de la Ley en particular lo dispuesto en el Inc. 2 del Art. 20, la responsabilidad del proveedor de aplicaciones de Internet por daños y perjuicios resultantes por uso de contenido generado por terceros, en caso de infracción de derechos de autor o derechos conexos, se seguirán rigiendo por la legislación de derechos de autor en vigencia previo a la fecha de entrada en vigencia de la presente Ley.

Art. 37. Esta Ley entrará en vigencia noventa días después de la fecha de su publicación.

Arequipa, 20 de Febrero del 2016

Anexo 1 E

FICHA DE JUICIO DE EXPERTO

ITEM	CONGRUENCIA		CLARIDAD		TENDENCIOSIDAD		Observaciones
	Sí	No	Sí	No	Sí	No	
¿De qué manera considera Ud. que se vulnera su derecho a la intimidad en las aplicaciones de Internet? a) Análisis de información íntima. b) Registro de comunicaciones. c) Limitaciones al derecho de defensa. d) Cambio de las políticas de privacidad. e) Por Espionaje.							
¿Conoce Ud. el tratamiento que realizan con sus datos íntimos las aplicaciones de internet? a) Destino desconocido de la información. b) Uso de información íntima. c) Control desigual de la información. d) Beneficio económico con datos íntimos.							
¿Cómo considera Ud. que son recogidos y almacenados sus datos íntimos por las aplicaciones de Internet? a) A través de perfiles de navegación online. b) Tráfico de datos. c) Registros obligatorios. d) A través de cuentas de internet.							
¿De qué forma cree Ud. que se garantice el derecho a la intimidad en las aplicaciones de Internet? a) Respetando la normativa nacional. b) Solicitando su consentimiento expreso.							

¿Qué tipos de protección a la intimidad le gustaría que implementen las aplicaciones de Internet para sus usuarios? a) Derecho al olvido b) Derecho de cancelación c) Notificar y retirar información d) Reparación de daños causados en Internet. e) Avisos de intromisiones.							