UNIVERSIDAD DE CHILE

Facultad de Derecho

Centro de Estudios en Derecho Informático

EL DERECHO AL ANONIMATO

DEL USUARIO DE INTERNET

Memoria para optar al grado de Licenciado en Ciencias Jurídicas

AUTORES: PATRICIO CABEZAS LOGAN

FERNANDO MOYA MUÑOZ

PROFESOR GUÍA: ALBERTO CERDA SILVA

-Santiago - Chile-
2008

ÍNDICE

Introducción.

La creciente vinculación de Internet con todas las actividades diarias hace que su uso sea cada vez más frecuente y necesario. Por lo mismo, su regulación se ha convertido en un elemento fundamental para el ordenamiento jurídico. Sin embargo, la naturaleza de Internet ha convertido esta regulación en un campo de difícil consenso, debido, principalmente, a las características particulares y únicas que presenta este medio de comunicación.

Básicamente, nos referimos a la rapidez, universalidad y libertad de los contenidos que pueden circular por la red. En este sentido, hay que pensar que un contenido que se encuentre en la Internet puede multiplicar su difusión en cuestión de segundos por el sólo objeto de recibir visitas o copias del mismo. Más aún, también Internet hace posible que un contenido permanezca en la red más del tiempo deseado, o dicho en otras palabras, que una vez en ella sea muy difícil su eliminación por completo.

Es por los motivos anteriores que los diversos ordenamientos jurídicos se han abocado a encontrar la manera de regular y vigilar el funcionamiento de la red. Sobre todo cuando se trata de proteger bienes jurídicos de orden superior, donde normalmente está involucrado un interés social o, incluso, mundial. Así sucede por ejemplo, con la protección que se hace en cuanto a los delitos comunes que se valen de Internet para su cometido. Pero esta labor también tiene sus barreras. De este modo, se debe tener siempre presente que Internet es un medio de comunicación.

Ello no sólo implica que se deban respetar las garantías mínimas dadas a cualquier medio masivo, sino que, además, debe tomarse en cuenta la facilidad que promueve la red en cuanto a sus costos y beneficios para sus usuarios. Así se plantea

como un medio universal que se ha desarrollado en gran medida en base a los bajos costos de ingreso y sus grandes beneficios en rapidez, eficiencia y calidad.

Se han suscitado, en este contexto, nuevos problemas que el derecho ha de responder. Nuevos desafíos que requieren adecuar las protecciones a las garantías fundamentales en este nuevo entorno virtual. La presente investigación trata el tema de la colisión de derechos que puede ocurrir al momento de enfrentar la privacidad de los usuarios de Internet versus el tratamiento de sus datos.

Si bien hasta hace algunos años atrás las actividades cotidianas de las personas no tenían directa relación con la red, en la época en que vivimos una porción sustancial de nuestras actividades cotidianas, como son el trabajo, los momentos de esparcimiento y ocio e, incluso, la interacción personal tienen lugar en el mundo virtual. Esto ilustra lo importante que resulta la protección de un derecho esencial que, hasta ahora, no se ha estudiado con la profundidad adecuada, nos referimos al derecho al anonimato.

Este trabajo pretende cuestionar hasta qué punto se pueden sacrificar los derechos del usuario en diversas hipótesis de riesgo. Se quiere analizar cómo y bajo qué circunstancias es posible intervenir las comunicaciones de las personas y guardar registros de las mismas. Si se cumple con guardar el registro de los inicios y términos de las comunicaciones o es admisible guardar un registro de los contenidos de dichas comunicaciones. Lo anterior teniendo como base el derecho al anonimato del usuario en la red.

Para efectos de nuestro análisis, partimos con una reseña histórica sobre los derechos de intimidad y privacidad, desde la comisión Ortúzar hasta conceptos doctrinarios de los mismos.

Posteriormente, nos enfocaremos al estudio del derecho al Anonimato, particularizando en su fundamento, contenido y expresiones normativas del mismo. Como se trata de una discusión de reciente data, creemos necesario hacer comparaciones con legislaciones extranjeras.

Para casos de estudios, haremos un análisis a la Ley de Pedofilía en cuanto a las obligaciones de guardar registro por los proveedores de acceso a Internet, y la Ley de Propiedad Intelectual, teniendo en cuenta el tratado de libre comercio con Estados Unidos, en lo relativo a la materia.

Con la finalidad de establecer el estándar de privacidad de los ISP, se establecerán hipótesis de riesgo, ya no sólo en relación a la investigación penal, sino a diversas situaciones que comprenden desde la perspectiva civil de la protección a la intimidad hasta las hipótesis contractuales.

Luego, analizaremos el conflicto que se da entre los diversos intereses que se pueden esgrimir para proceder a establecer registros y los derechos fundamentales de los usuarios, ya sea de intimidad, privacidad o autodeterminación informática. Finalmente, se harán conclusiones en base a una visión crítica a la legislación actualmente vigente en nuestro país y a los planteamientos de la doctrina y jurisprudencia.

Capitulo I.

Derechos de los usuarios.

1. Derecho a la Intimidad y Privacidad.

1.1 Origen Histórico.

La mayoría de los ordenamientos jurídicos modernos contempla en su carta fundamental un apartado dedicado al resguardo que el Estado debe prestar a la vida privada. En este sentido, se consagran valores como la protección a la intimidad, la honra y la propiedad privada. Conceptos distintos, pero muy relacionados y que trataremos de ir analizando poco a poco. Son ideas que nacen desde temprano en la época moderna, sin embargo, no es sino a comienzos del siglo pasado donde se forma el consenso sobre la necesidad de su regulación jurídica.

En este apartado analizaremos brevemente la evolución que el derecho a la vida privada ha tenido en los principales regímenes que conciernen a nuestra cultura jurídica occidental. Pasando por la evolución en los Estados Unidos y Europa como sus primeras manifestaciones, para luego revisar la posición internacional y regional.

De este modo debemos partir haciendo reseña a uno de los lugares donde este concepto más se ha ido desarrollando, en los Estados Unidos de América. Tanto debido a la cultura como a la posición pionera en el resguardo de las libertades civiles y políticas, este país se ha convertido en un referente obligado al momento de analizar la evolución de las políticas de protección a la vida privada. De hecho, ya en la cuarta enmienda de la Constitución de los Estados Unidos se señala el derecho a la seguridad en la persona, su hogar, papeles y efectos personales, y contra búsquedas irracionales

protegiendo la inviolabilidad[1]. Conceptos que dan la base a lo se puede definir como el bien jurídico protegido.

De manera más concreta, el profesor Eduardo Novoa Monreal nos señala que: *"El llamado "derecho a la vida privada" surge de manera especifica en los Estados Unidos, en 1890…. Poco antes el juez norteamericano Cooley había proclamado el "derecho a ser dejado tranquilo y de no ser arrastrado a la publicidad" como lo propio del derecho a la intimidad.*

Sin embargo, la jurisprudencia norteamericana rechaza el concepto inicialmente. Después, empieza a reconocerlo en forma gradual, pero con formas y fundamentos divergentes de las que hoy son más generalmente aceptadas"[2].

Es decir, las ideas de privacidad contenidas en principios generales no contaban con un arraigo generalizado en la población. Debemos recordar que la democracia moderna como hoy la conocemos estaba aún en ciernes, y como tal los derechos de las personas con un incipiente resguardo.

En tanto, a nivel europeo países como Italia, Alemania y Francia han enfrentado de diversas maneras el tema. De este modo hacia la década de los setenta, *"la doctrina y jurisprudencia en Francia habían adelantado bastante en la creación jurídica del concepto"*[3]. Con enfoques distintos, lo acercaban más a lo que se denominaría el derecho de la personalidad. Como tal, el derecho a la vida privada gozaría de un reconocimiento parcial en la medida que se encuentre vinculado con el derecho antes mencionado. Incluso en países como Alemania, donde durante mucho tiempo se discutió

---

[1] *The Constitution of the United States of America, IV Amendment.* En ROSSITER, Clinton (ed), *The Federalist Papers,* Mentor, New York, 1999. Pág. 522. El texto original dice asi: " The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, or particularity describing the place to be searched, and the persons or things to be seized."

[2] NOVOA, Eduardo. *Derecho a la vida privada y la libertad de información: Un conflicto de derechos.* Editorial Siglo XXI, México, 1997, p. 26.

[3] Ibíd. p. 26.

la existencia del derecho a la personalidad, la ley suprema de 1949 concede los caminos necesarios para que los tribunales apliquen el derecho a la vida privada como parte de los derechos de la personalidad.

Pero también a un nivel internacional el derecho a la vida privada ha tenido una evolución sostenida. Así es como en la Declaración Universal de Derechos Humanos de 1948 se consigna la garantía a no ser objeto de injerencias arbitrarias en la vida privada. Se reconoce y postula el concepto de "arbitrariedad" como elemento del cual la vida privada se protege. En otras palabras, lo que se busca señalar es la diferencia con la intervención legítima en la vida privada. Ello como parte de la acción del Estado en resguardo de otros derechos que la comunidad ha decidido preservar y a los cuales se les otorga un valor preponderante en sociedad, a tal modo que lleva a sacrificar los derechos individuales que se han protegido.

A nivel regional, la Convención Americana de Derecho Humanos también protege el derecho a la vida privada de manera similar a lo señalado anteriormente. En este caso se incluye dentro del derecho a la dignidad de la persona. Así su artículo 11 señala[4]:

Protección de la Honra y de la Dignidad

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.

[4] Convención Americana sobre Derechos Humanos, "Pacto de San José de Costa Rica". Organización de Estados Americanos, en Internet, http://www.oas.org/juridico/spanish/firmas/b-32.html (última visita Octubre de 2004)

En todos los casos señalados anteriormente, se observan garantías que pueden permitir que las personas gocen de su vida privada en el resguardo más íntimo de su círculo. Pero a la vez cabe constatar que debido a la época en la cual estos documentos fueron realizados, las aproximaciones del tipo más concretas sólo hacen referencias a correspondencia, papeles o documentos. Por lo tanto, las referencias explicitas a la vida privada en el ámbito digital, sólo las encontraremos en la legislación más moderna.

En Chile, la expresión normativa de estos Derechos se encuentra en el artículo 19 Nº 4 de la Constitución Política que señala la garantía de *"El respeto y protección a la vida privada y a la honra de la persona y su familia"*[5]. Además su protección en particular se encuentra determinada por variadas leyes y normativas jurídicas, las cuales se analizarán en profundidad en el avance del trabajo, por consistir, en sí mismas, el marco jurídico base del análisis.

El Concepto en la comisión Ortúzar.

En la discusión de la comisión Ortúzar se expresó por parte del Señor Guzmán *" que es importante – y así ha dicho en sesiones anteriores de la Comisión- destacar la introducción de 2 valores distintos de la inviolabilidad del hogar y de la correspondencia en la forma tradicional que se consagraba, y que son los que el señor Silva Bascuñan en su proposición procura establecer a través de los términos respeto a la intimidad y al honor de las personas. Piensa, sin embargo, que el primer concepto se expresa en forma más adecuada y completa en la noción de privacidad, porque ésta envuelve el ámbito de una zona de la vida de la persona que debe quedar precisamente excluida de la noticia o de la invasión externa.*

[5] Ley Nº 20.050 Art. 1º nº 10 letra b) que modifica Constitución Política de la República, D.O 26-08-2005.

La intimidad, continua, es todavía una zona más profunda y sensible que la privacidad. Es algo todavía más sutil y, por lo tanto, de menor alcance en su extensión. Enseguida, expresa que lo anterior tiene una trascendencia bastante grande y habrá que hacer algún tipo de relación sobre el punto cuando se trate el tema de los medios de comunicación, sin perjuicio de que en esta materia , ya sea referido a los medios de comunicación o a otras manifestaciones en que el consagrar este derecho puede adquirir una importancia práctica muy grande , va a ser la jurisprudencia la que en definitiva irá calibrando o precisando a quién y hasta dónde alcanza este derecho la privacidad"[6].

Lo anterior, es la idea de que el Derecho debe garantizar a cada individuo una zona privada para el mejor desarrollo de su personalidad. Es la concepción liberal de la intimidad, entendida básicamente como una libertad negativa[7]. "*La esfera privada se dibuja como un bastión de no interferencia en lo que sería el último reducto de la libertad"*[8].

La comisión señala, a su vez, que será la jurisprudencia la que establecerá los límites a la privacidad, así señala Guzmán, "*en cuanto a que se fije por la jurisprudencia los limites, le parece que va a ser inevitable que así sea. No cree que la Constitución pueda, al tratar de los medios de comunicación ser demasiado precisa en cuanto hasta dónde se extiende el ámbito de la privacidad, porque es evidente, por ejemplo, que la persona que actúa en la vida pública deba entender, en su opinión, que cierta parte de su vida privada está puesta en tela de juicio en una mayor medida que la de una persona que jamás ha intentado actuar en la vida pública. (...)El señor Diez desea dejar constancia en la Actas de la Comisión que la privacidad, la honra y el*

[6] Actas Oficiales de la Comisión Constituyente, sesión 129, celebrada el día 12 junio de 1975. p. 23.
[7] CORRAL, Hernán , "Derechos al honor, vida privada e imagen y responsabilidad civil por los daños provocados por las empresas periodísticas", Revista de Derecho, Universidad Católica de la Santísima Concepción, volumen V. p. 79.
[8] BEJAR, Helena , El ámbito íntimo. Privacidad, individualismo y modernidad, Editorial Alianza S.A., Madrid, 1988, pp. 26-28.

respeto a la vida familiar de las personas, no sólo dicen relación con los medios de comunicación social, sino, también, con otros aspectos de la vida pública, ya sea administrativa o política, e incluso, con la responsabilidad de aquellos que tienen ciertas inviolabilidades en razón de los cargos que detentan. También afirma que la garantía del respeto a la vida privada de la persona cubriría también la posibilidad de captación de imágenes. Esto, para ir extendiendo el sentido, alcance y proyección del precepto que se está aprobando"[9].

El sentido y alcance se extiende, ya no es entendida como libertad negativa. "*En la actualidad, la intimida conserva su núcleo de libertad negativa, y absorbe una dimensión positiva, que confiere al sujeto el poder de tomar decisiones y conducir su vida sin verse determinado por la voluntad de otros*" [10].

Así es como vemos que en los distintos ordenamientos jurídicos, desde temprano en la historia moderna, la vida privada se ha ido manteniendo como objeto de protección jurídica. Entonces el problema no reside tanto en su defensa y protección, por el contrario, el principal conflicto depende de qué se entiende por vida privada.

1.2 Conceptos de Derecho a la vida privada e intimidad.

La mayoría de la doctrina nacional como extranjera se inclina por no dar definiciones cerradas sobre lo que es la vida privada[11]. Ello es de suma lógica al entender que es un derecho que evoluciona con el tiempo de las sociedades. En la edad media, posiblemente, no se consideraría de la esfera de la vida privada lo que el vasallo tuviese en su morada frente al rey. Hoy sin embargo, la inviolabilidad del hogar se constituye como uno de los pilares de la vida privada.

[9] Actas Oficiales de la Comisión Constituyente, Op. cit. pp. 22-23.
[10] ZÚÑIGA, Francisco, "El derecho a la intimidad y sus paradigmas". Ius et Praxis, Derecho en la Región, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, año 3 Nº 1, Talca , 1997, p. 288.
[11] CORRAL, Hernán, Op. cit., p. 75 y Zuñiga, Francisco, Op.cit. pp.285-290.

Otro ejemplo de lo variable en el tiempo que resulta la vida privada es el hecho que hoy abarca zonas no previstas con anterioridad, así el avance de la tecnología y la informática hace surgir el concepto de libertad informática. Ella conjuga tanto el aspecto negativo tradicional de la privacidad, esto es, exclusión de terceros del ámbito de lo íntimo con una libertad positiva de control de la información, que también se denomina autodeterminación informática[12]. De ahí que además, de las complejidades propias del término, se suma el problema de la adaptabilidad que debe tener en cuanto a los avances de las sociedades.

En este sentido, el profesor Novoa Monreal nos señala una serie de conceptos que diversos estudiosos del derecho que muestran cómo la vida privada está lejos de suscitar consenso en su definición[13]. Por lo mismo, compartimos sus ideas al decir que *"no existe un concepto único de vida privada, se trata de algo relativo y, por consiguiente, variable conforme a ciertas condiciones"*[14]. Lo mismo hace que, al esbozar un concepto, sólo se busque plantear ideas generales acerca de lo que es el derecho a la vida privada.

La vida privada es todo lo cual se quiere mantener fuera del conocimiento público, respecto a lo cual existe cierto consenso social y cultural dependiendo de cada país y época. La referencia al ámbito público debe entenderse como la esfera del dominio común en las relaciones sociales. En este sentido, lo público es lo que cualquier persona puede conocer ejercitando los mínimos derechos que en un ordenamiento jurídico se conceden. Luego, señalamos que provoca cierto consenso, ya que es imposible que los elementos que comprenden la vida privada sean uniformemente aceptados. Aún dentro de un contexto social y cultural determinado, existen posiciones

[12] PEÑA, Carlos, "El Derecho Civil en su relación con el derecho internacional de los derechos humanos, Cáp. VIII, Sistema Jurídico de derechos humanos, en Cuadernos de Análisis Jurídico, Serie Publicaciones Especiales Nº 6 (Cecilia Medina y Jorge Mera editores), Universidad Diego Portales, 1996, pp. 584-585.
[13] Ver NOVOA, Eduardo, Op. cit. p.35 y siguientes.
[14] *Ibíd.* p. 42.

más conservadoras y otras más liberales que seguramente diferirán de lo que merece ser protegido como esfera de la vida privada. Sin embargo, al igual que conceptos abstractos como buenas costumbres o moral pública, hay ideas generales que sí son mayormente consensuadas.

Referente a lo anterior, una sociedad puede generar ideas consensuadas en la medida que su elección escuche a todos los miembros de la misma, o en su defecto, a todo grupo que represente a una parte de ella, por minoritario que sea. Pero además, cuando este consenso puede y lleva a permitir una mayor paz social. En base a ello, podemos entender que la vida privada es lo que se quiera mantener fuera del ámbito público, considerando los aspectos relativos a ideas de tipo personal – como religión, orientación sexual, política, etc.…- de salud o físicas, comunicaciones personales y "*en general, todo dato, hecho o actividad personal no conocidos por otros, cuyo conocimiento por terceros produzca turbación moral o psíquica al afectado"*[15].

En esta base, se da paso a otro concepto relacionado: el de intimidad. Nos señala el profesor Nogueira: *"La vida privada en un circulo o ámbito más profundo lleva al concepto de intimidad. La intimidad es el ámbito reservado del individuo que no desea ser develado al conocimiento y acción de los demás, el cual aparece como necesario para mantener un mínimo de calidad de vida humana. El derecho a la intimidad es la facultad de la persona para evitar las injerencias de terceros en el ámbito de su privacidad, salvo la autorización de tal develamiento de la intimidad por el propio afectado"*[16].

Hay autores que utilizan como sinónimos los conceptos de intimidad y privacidad, entre los cuales Novoa Monreal señala que no se advierte la necesidad de

[15] Ibíd. p. 46.
[16] NOGUEIRA, Humberto. "El Derecho a la libertad de opinión e información y sus limites: honra y vida privada". Ed. Universidad de Talca y Lexis Nexis. Santiago de Chile, 2002. p. 147.

hacer una diferenciación entre lo privado y lo íntimo[17], como también en el mismo sentido José Luis Cea señala que la vida privada busca asegurar el Derecho a la Intimidad[18]. Pese a estas opiniones consideramos que no son sinónimos, y para claridad conceptual adoptamos la distinción que realiza Humberto Nogueira.

De este modo, dentro de la intimidad, se sitúan los aspectos más sensibles de la vida privada. Las creencias de la persona, aquellas que ésta ha decidido mantener para sí o en su entorno más intimo. La protección de los datos que una persona da a una institución determinada es objeto del derecho a la vida privada si sólo han sido consentidos para esa institución. Pero no es lo mismo cuando los datos de esa persona se ponen frente a frente, con la comunicación que se hace por un individuo de su condición de salud a sus familiares.

Se comprende entonces que la vida privada contiene los aspectos más sensibles de la vida de una persona. Son aspectos que no se quiere que sean conocidos. Por lo mismo, su revelación provoca un daño en la persona que va ligado a otros derechos esenciales del ser humano como el derecho a la dignidad y a la honra.

En efecto, aspectos centrales del derecho a la vida privada pueden relacionarse con el mantener el deber de secreto o resguardo de las comunicaciones. Así, hay veces que la persona ha hecho uso de su derecho de dar a conocer cierta parte de su intimidad, de manera libre y espontánea, con el correlativo deber de secreto de la contraparte. Otras veces, sin embargo, la persona no manifiesta esta intención en aspecto alguno de su vida privada. No estamos entonces dentro del aspecto del deber de secreto, sino del aspecto de no involucrarse en lo que no desea ser comunicado. Es el campo del derecho al anonimato que se examinará con mayor atención en el siguiente apartado.

[17] NOVOA MONREAL, Eduardo. Op. cit. p. 47.
[18] CEA, José Luis, "El Derecho Constitucional a la Intimidad." Revista Gaceta Jurídica Nº 194. Editorial Conosur. 1996.

2. Derecho al Anonimato.

2.1 El Anonimato en la Red.

Internet es considerado como un medio para la libertad, debido principalmente a que los sujetos pueden difundir libremente sus ideas. Este paradigma tiene un fundamento tecnológico, como lo señala Manuel Castells,[19] el cual es que su arquitectura basada en la conexión informática en red sin restricciones, sobre protocolos que interpretan la censura como un fallo técnico y simplemente la sortean dentro de la red global, hacen que sea bastante difícil controlarla. En este plano, cabe preguntarse cómo se encuentra protegida la Privacidad de los usuarios. "*Los usuarios encuentran protección a su Privacidad por el anonimato de la comunicación en Internet, como también por la dificultad de rastrear las fuentes e identificar el contenido de los mensajes transmitidos por medio de los protocolos de Internet"*[20]. Esta circunstancia fáctica es la primera aproximación que tenemos a lo que es la expresión de un Derecho Fundamental aplicado al mundo virtual. Hay que dejar en claro que no es la circunstancia fáctica técnica la que es digna de tutela jurídica, sino que la protección va encaminada al usuario, para la protección de su dignidad como persona.

Hay una corriente de opinión que considera negativo el hecho del anonimato en la red. Esta opinión se refleja en el denominado caso ENTEL. El año 1999 se recurre contra la empresa ENTEL porque en una de sus direcciones apareció un aviso de ofrecimientos sexuales, en la que figuró como remitente una menor de edad. De acuerdo a lo que señala la parte recurrente "*la actitud (de ENTEL) importa absoluta arbitrariedad, pues ha permitido irresponsablemente la publicación del aviso y otros de similar naturaleza por parte personas* ***anónimas*** *sin verificar la identidad de sus fuentes, contribuyendo a que mentes desquiciadas utilicen el sistema atropellando la*

[19] CASTELLS, Manuel, "La Galaxia Internet", Editorial Areté, Barcelona, 2001, p.195.
[20] Ibíd. p. 193.

integridad física y psíquica de las personas". Continua el argumento de la parte recurrente señalando que "*que la acción de ENTEL S.A. de poner un funcionamiento un sistema que permite la expresión de conceptos dañosos por parte de personas anónimas y la publicidad de ofrecimientos sexuales aberrantes constituye una acción arbitraria como también lo es la omisión de no verificar la identidad de sus fuentes, dejando en la indefensión a las personas que carecen de medios para asegurar el respeto de sus derechos"*[21]. Este tipo de opinión adolece del error de considerar que el mundo del ciberespacio posee las mismas características que el mundo del espacio real.

Para explicar, las diferencias tomamos como punto de referencia a Lessig, en cuanto él llega a la conclusión que en el mundo del espacio real el anonimato ha de crearse mientras en el ciberespacio el anonimato viene dado de antemano[22] . Para esto utilizamos 2 conceptos, identidad y autenticación. Se entenderá identidad en un sentido amplio, como todos los hechos ciertos acerca de una persona, donde se incluyen sexo, nombre, profesión, gustos, etc. En cambio, autenticación es un proceso por el cual se revelan algunos aspectos de la identidad de una persona.

En el mundo real "*una buena parte de nuestra identidad queda develada independiente de nuestra voluntad"*[23] , esto se explica a través de ejemplos, uno al caminar por un paseo peatonal, o al dirigirse a realizar algún trámite a una oficina, quedan develados para los demás sujetos que interactúan con uno algunos hechos que configuran la propia identidad. Así, los demás sujetos sabrán el color de pelo de uno, el sexo, la forma de vestir, color de piel, etc. Para que puedan pasar desapercibidos estos hechos la persona tendría que disfrazarse u ocultarse (crear al anonimato) lo cual no sería muy lógico. Otros hechos que configuran la identidad no son develados tan rápidamente y es necesario autentificarlos, para ello están las credenciales o certificados.

[21] Sentencia de 6 de diciembre de 1999 de la Ilma. Corte de Apelaciones de Concepción recaída en el Recurso de Protección interpuesto por Orlando Fuentes Siade contra ENTEL S.A., rol Nº 243-99.
[22] LESSIG, Lawrance, "El código y otras leyes del Ciberespacio". Editorial Grupo Santillana de Ediciones, Madrid, 2001.p. 72.
[23] Ibíd. p. 68.

En una oficina pública para algún trámite se exigirán cédula de identidad, certificado de nacimiento, entre otros. Estos certificados o credenciales son respaldados por una institución que las otorga. Así la identidad en el espacio real se determina, por una parte, por hechos que se revelan automáticamente y otros que requieren un proceso de autentificación.

En el ciberespacio, la situación difiere sustancialmente por cuanto, en el plano de la identidad, lo único que se tiene es un número IP. "*Los protocolos sobre los que se basa Internet, sin embargo no revelan información alguna acerca de la persona que se conecta a la Red ni acerca de las datos que ésta intercambia"*[24], es así, que no se obtiene información acerca del usuario por medio del protocolo en sí mismo. En el plano de la autentificación el ciberespacio tampoco revela ningún hecho autentificador[25]. Así, el anonimato en la red viene dado de antemano por la arquitectura de Internet, lo que no implica que vaya a ser así por siempre. Son expresivas las palabras de Lessig en cuanto a que en la Red "*es tan fácil ocultar que eres un perro como difícil probar que no lo eres"*[26]*,* y aquello se presenta como un problema para el comercio en Internet.

2.2 Concepto de Derecho al Anonimato.

La aparición del concepto de Intimidad se liga con el nacimiento de la burguesía y la desintegración del sistema feudal, y el Derecho a la privacidad encuentra sustento teórico en la idea de libertad individual de John Stuart Mill y luego en el trabajo de Samuel Warren y Luis Brandeis en 1890, donde se establece que dadas las nuevas condiciones de la vida moderna las personas deben tener una real protección a la esfera de su intimidad[27]. De la misma manera que la Intimidad tiene su génesis con la aparición de la burguesía y la privacidad en el surgimiento de la modernidad, en el caso del

[24] Ibíd. p. 70.
[25] Es por eso que el comercio aboga por el desarrollo de "arquitecturas" que permitan la identificación y posterior autentificación del sujeto, esto principalmente a través de certificados digitales.
[26] LESSIG, Lawrence, "El código y otras leyes....", Op. cit. p. 72.
[27] PEÑA, Carlos, Op. cit. p. 580.

Derecho al Anonimato, en los términos que aquí lo vamos a conceptuar, tiene su origen con Internet.

El Derecho al Anonimato no es un concepto indeterminado pero si puede ser considerado un concepto difuso. Esto porque puede resultar más conveniente su caracterización antes que una determinación a priori. En este sentido se manifiesta el Profesor Carlos Peña al señalar que la privacidad o la intimidad, es un concepto difuso, esto por dos sentidos: primero, porque su determinación es inconveniente a priori, debiendo buscarse su caracterización mejor en el estudio de las lesiones que hayan obtenido una legitimación paradigmática en la práctica jurídica cercana como lesiones del derecho a la intimidad, o bien una conceptualización positiva, como derecho de participación o libertad positiva, en base a un rasgo común; segundo, en el sentido de que los problemas que plantea la privacidad se expanden con la tecnología también[28].

De esta manera, podemos señalar que el Derecho al Anonimato se puede conceptualizar como el derecho que tiene el usuario de Internet para que su identidad permanezca oculta o en forma reservada ante la mirada de otros actores que se desenvuelven en la Red. El contenido del Derecho al Anonimato incluye la confidencialidad de las comunicaciones en Internet, la confidencialidad de los datos de tráfico y de todos aquellos datos e informaciones que permitirán desenvolverse con la mayor libertad en la Red. Así, el Anonimato se presenta como necesario para el desenvolvimiento en la red.

Un Derecho se justifica por su capacidad para promover ciertos bienes básicos para las personas como son la libertad o la igualdad, entre otros.

En el caso del Derecho al Anonimato su justificación esta dada por permitir el libre desarrollo de la persona, que no es otra cosa que la posibilidad de elegir lo que uno

[28] Ibíd. p. 581.

puede hacer con su vida aplicado al ámbito de Internet. Su autonomía conceptual, con respecto a la privacidad, está dada porque los niveles de protección al usuario en uno y otro concepto difieren. En el mundo virtual, el Derecho al Anonimato permite la protección del usuario en su esfera privada. Puede suceder que un usuario decida renunciar, en una situación determinada, a su Anonimato, sin embargo no por ello está renunciando a la protección de una esfera privada.

Es necesario hacer referencia que el Derecho al Anonimato comprende por una parte la confidencialidad de las comunicaciones electrónicas como también el respeto a los datos de tráfico en Internet, respeto a los datos de localización que no sean datos de tráfico y un buen tratamiento de las facturas desglosadas. Estas son las principales hipótesis de configuración normativa del anonimato que se da en el ámbito comunitario. A modo de ejemplo para hacer presente la importancia del Anonimato en la Directiva 2002/58 sobre los datos de tráfico se señala que *"deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación"*[29].

2.3 Fundamento de la existencia del Derecho al Anonimato.

Hasta hace algunos años atrás las actividades cotidianas de las personas no tenían directa relación con la red. En cambio, en la época en que vivimos una porción sustancial de nuestras actividades cotidianas, como son el trabajo, los momentos de esparcimiento y ocio e incluso la interacción personal tienen lugar en el mundo virtual

[29] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de las Comunidades Europeas.* 31 Julio de 2002. Artículo 6, Datos de Tráfico 1. Sin perjuicio de los dispuesto en los apartados 2,3 y 5 de l presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al publico deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.

de la red. Esto sirve para ilustrar lo importante que resulta la protección del Anonimato para que el sujeto se pueda realizar libremente como persona.

De esta manera, la vida moderna se plantea como un híbrido de interacción on line e interacción física, así en palabras de Manuel Castells *"la vida en un sistema electrónico sin privacidad implica que la mitad de nuestras vidas esté permanentemente expuesta a la vigilancia. Como vivimos existencias compuestas, se puede derivar en una existencia esquizofrénica de acuerdo a la cual seríamos nosotros mismos off line y una imagen de nosotros mismos on line, con lo que se internaliza la censura"*[30].

Lo que resulta preocupante en torno al Derecho al Anonimato es la ausencia de reglas explícitas de conducta y el qué terceros puedan juzgar nuestro comportamiento con las consecuencias nefastas que acarrea, así son expresivas las palabras de Luis García San Miguel cuando señala que "*si alguien nos mira nos juzga y, cuando nos juzga, en cierta medida nos domina*"[31] y así Internet pasaría de ser el paradigma del espacio de libertad para convertirse en una casa de cristal[32].

Por otro lado, Antonio Enrique Pérez-Luño nos señala que en la sociedad contemporánea *"la injerencia del ordenador en las diversas esferas y en el tejido de relaciones que conforman la vida cotidiana se hace cada vez más extendida, más difusa, más implacable. Por ello resulta cada vez más apremiante el reconocimiento del derecho a la libertad informática y a la facultad de autodeterminación en la esfera informativa"*[33]. Junto a estos reconocimientos agregamos el Derecho al Anonimato.

---

[30] CASTELLS, Manuel, "La galaxia...", op. cit. p. 206

[31] GARCIA SAN MIGUEL, Luis, "Estudios sobre el Derecho a la Intimidad". Editorial Tecos Universidad de Alcalá de Henares, Madrid, 1992 p. 9.

[32] CASTELLS, Manuel, "La galaxia...", op. cit. p. 204.

[33] PÉREZ LUÑO, Antonio, **"**Del Hábeas Corpus al Hábeas Data" Editorial Aranzadi, Madrid 1991, p.194.

Ahora, la existencia del derecho del anonimato puede generar controversias en cuanto a su delimitación. Para otorgar claridad al respecto, es necesario previamente abordar la ubicación sistemática que le daremos al Derecho al anonimato. La problemática de ubicar sistemáticamente un nuevo derecho se produjo con anterioridad al tratar las leyes de protección de datos personales y el surgimiento del derecho a la autodeterminación informática. Es así que se ha señalado que ante la protección de la persona por el tratamiento automatizado de datos personales se está frente a la existencia de un nuevo derecho fundamental, que corresponde al de la libertad informática o autodeterminación informática.

Frente a lo anterior, la pregunta es si estamos en presencia del surgimiento de un nuevo derecho de la personalidad. Una respuesta es que si estemos en presencia de un nuevo derecho. En ese caso habría que delimitar la relación que existe con el derecho fundamental correspondiente. Si la respuesta fuera negativa se trataría que la normativa en cuestión de protección del tratamientos automatizado de datos personales es protectora de derechos de la personalidad, ya existentes, como sería la intimidad. Sin ahondar en las relaciones existentes entre los derechos de la personalidad y los derechos fundamentales, debemos dejar sentado que en el caso que tratamos existe la situación en que un derecho de la personalidad, es a la vez, un derecho fundamental.[34] El hecho de mantener una perspectiva que manifieste las diferencias conceptuales con un mero afán de atribuirse el estudio de estos derechos no tiene cabida, toda vez que para poder rellenar insuficiencias en torno a los derechos de la personalidad, se deberá poner atención al régimen de los derechos fundamentales incluidos en las cartas internacionales de Derechos Humanos.

La misma situación ocurre con respecto a la utilidad que presentan los derechos de la personalidad para el estudio de los Derechos Fundamentales. Es así como Ortí

[34] ORTÍ VALLEJO, Antonio, "*Derecho a la intimidad e informática : (tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales, particular atención a los ficheros de titularidad privada",* Editorial Comares, Granada , España, 1994, pp.24-25

Vallejo señala que *"ambas categorías se requieren mutuamente"*. En el ámbito del presente trabajo lo que realmente interesa es que el derecho en cuestión, el anonimato, más allá de referirse a un derecho fundamental o de la personalidad implica un mismo bien jurídico protegido: *"el derecho de la personalidad no pierde su carácter por el hecho de recibir consagración constitucional sino que sin dejar de ser derecho de la personalidad adquiere a la vez naturaleza de derecho fundamental. Se trata conceptualmente del mismo derecho"*[35]. En definitiva, implica adoptar una perspectiva unitaria, ya que esta se presenta como favorable para un estudio más enriquecedor, así *"un criterio unitario rechaza el mantenimiento tajante para estos derechos de conceptos y metodologías distintas, pues se trata de fenómenos jurídicos que ontológicamente, sólo tienen una respuesta: constituyen las prerrogativas más elementales de la persona humana en las sociedades civilizadas. En otras palabras, los conceptos de derechos fundamentales y de derecho de la personalidad no son excluyentes, sino convergentes"*[36].

Luego es necesario hacer una distinción en lo referente a sus realidades como derechos considerados a ser protegidos y su relación histórica en la clasificación de derechos fundamentales o de la personalidad.

El problema consiste en determinar si es posible introducir por vía interpretativa nuevos derechos fundamentales o derechos de la personalidad. Este problema fue tratado al determinar si era posible introducir un derecho a la autodeterminación informática. Al respecto Ortí Vallejo señala que "*si, se pueden crear derechos de esta índole"*[37], en base a una recalificación de los derechos en una categoría histórica. Es posible tanto en el caso de los Derechos Fundamentales como en los Derechos de la Personalidad. PÉREZ LUÑO afirma que lo que sean los Derechos Humanos "*tan sólo puede predicarse con sentido en contextos temporalmente determinados (…..) Hay que*

[35] Ibíd. p.27
[36] Ibíd. p 29.
[37] Ibíd. p. 31.

reemplazar el enfoque intemporal de los Derechos Humanos, tendente a contemplarlos como categorías cerradas y definitivas, por una visión histórica que los conceptúe como respuestas a las necesidades humanas y a las distintas modalidades de amenaza y agresión a los seres humanos que se suceden en el tiempo"[38].

La misma recalificación jurídica basada en el plano histórico se efectúa respecto a los Derechos de la Personalidad, citando a López Jacoiste, Ortí Vallejo señala que *"se considera a los derechos de la personalidad una categoría que se encuentra en incesante evolución y que cambia en cuanto a la formulación de los ya existentes, cuando, merced al flujo histórico, cambian los ámbitos probables y las dimensiones de la proyección de la persona"*[39].

Al respecto vale la pena preguntarse cuándo es posible afirmar la existencia de un nuevo derecho. Para ello López Jacoiste afirma que *"sólo cuando las circunstancias que aconsejen su implantación alcancen un relieve diferenciado y propio, socialmente consolidado y apreciado, estarán sentadas las bases de un derecho nuevo"*[40]. Consideramos que respecto al derecho al anonimato, ahora existe dicho carácter diferenciado basado en la creciente masificación del uso de las nuevas tecnologías que las han sacado del ámbito exclusivo de las aulas universitarias o recinto militares.

Hoy, la mundialización de las redes y las nuevas tecnologías hace que este derecho alcance una estatus social que debería poseer un lugar dentro de los distintos ordenamientos jurídicos. La crítica está dada por cuanto los derechos de la personalidad o fundamentales llamados clásicos están asentados hace más tiempo que este nuevo Derecho al anonimato, luego sería mejor seguir tratando con categorías jurídicas como la privacidad o la intimidad, que ya se encuentran afianzadas en el ordenamiento

[38] PÉREZ LUÑO, Antonio, "Los derechos humanos en la sociedad tecnológica", Cuadernos y Debates, 21, Centro de Estudios Constitucionales, Madrid, 1989, p. 142.
[39] LÓPEZ JACOISTE, José Javier citado por ORTÍ VALLEJO, Antonio Op. cit. pp. 32-33.
[40] Ibíd. p. 34.

jurídico. Pensar de esta manera implica admitir que nada cambia, es una configuración estática del mundo, incluso el hecho de analizar esas categorías jurídicas pensando en intentar adecuarlas forzándolas, no nos parece acertado.

Lo anterior es esbozado por Lessig al señalar que *"la cuestión no estriba en si existía ya algo como lo que hay en la actualidad sino si lo que ocurre hoy es sustancialmente diferente. (...) Si es diferente, entonces debemos preguntarnos si debemos tratarlo de manera diferente"*[41]. Expresivo al respecto es el ejemplo que pone el mismo autor al señalar que el gato y el tigre son parecidos, pero el tigre no es un animal doméstico, luego no es nuestro planteamiento que el mundo surgido por la aparición de Internet sea un mundo salvaje, sólo plantear la necesidad de afianzar la categoría jurídica del Derecho al anonimato, como categoría independiente de la privacidad e intimidad.

Ahora, las implicancias prácticas del alcance jurídico del derecho al anonimato aún pueden ser difusas. En este sentido, el derecho al anonimato aún no es unánimemente aceptado en materia jurisprudencial, por lo mismo puede carecer de la fuerza necesaria para una adecuada defensa de los intereses que el mismo derecho protege. En otras palabras, debido a la incipiente – y aún no cerrada – discusión acerca de la naturaleza jurídica del derecho del anonimato, aún será conveniente ceñirse a conceptos más ampliamente aceptados en el quehacer jurídico, como el derecho a la privacidad o intimidad a la hora de recurrir a nuestros tribunales por la defensa de nuestras garantías.

Pero ello no implica que, para otros efectos jurídico político el derecho al anonimato se esté consolidando y sea de útil aplicación. Así como la privacidad "*se trata de una garantía básica para cualquier comunidad de los ciudadanos libres e*

[41] LESSIG, Lawrence, "El código y otras leyes...", Op. cit. p. 278.

iguales"[42]*,* el anonimato es una garantía básica para lo que podemos denominar la comunidad virtual.

2.4 Contenido del Derecho al Anonimato.

Para analizar el contenido del derecho al anonimato es necesario primero hacer una breve distinción entre los distintos bienes jurídicos que se podría involucrar. De este modo se pueden señalar: la inviolabilidad de las comunicaciones, la privacidad en general y la autodeterminación informática.

El contenido del derecho al anonimato tiene que ver con la protección de bienes jurídicos determinados. Tal como lo señala Jakobs *"todo bien jurídico necesita para realizar las potencialidades en él contenidas de una serie de condiciones acompañantes, y hoy en día ya no se da por supuesto que estas condiciones concurran, ni tampoco que sea un destino ineludible el que falten. (...) Dicho en el lenguaje de la protección de bienes: no sólo los bienes jurídicos clásicos son bienes escasos, sino que conforme al entendimiento actual lo son también sus condiciones de utilización"*[43].

Para graficar lo anterior, nos ponemos en la siguiente situación hipotética; si se crease una ley contra el monitoreo informático de las personas, en un mundo donde no hubiera existido la informática o donde esta no sea masiva, dicha ley no hubiese tenido ningún sentido. De la misma manera, no cabría cuestionarse la existencia del Derecho al Anonimato sin Internet. En el mundo actual, el derecho al anonimato nos es útil para resguardar bienes jurídicos clásicos. Así, si hay una ley contra el monitoreo, se podrían llegar a proteger el bien jurídico de la inviolabilidad de las comunicaciones, de la privacidad y de la autodeterminación informática.

---

[42] Ibíd. p. 65.
[43] JAKOBS, Gunther, *"Sociedad, norma y persona en una teoría de un derecho penal funcional"*, Editorial Civitas, Madrid, 1996, p. 45.

El derecho al anonimato tiene una autonomía conceptual, pero a la vez es funcional a la protección de los bienes jurídicos clásicos. Entonces el derecho al anonimato, siguiendo en la categoría de Jakobs, se construye por una serie de condiciones acompañantes, como condición necesaria que a su vez brindan protección en el ámbito de la informática a los otros bienes jurídicos mencionados.

En este análisis del contenido del derecho al anonimato, es posible aún verlo como un derecho de contenido difuso. Crítica que puede ser bien fundamentada debido a la imprecisión del término. Sin embargo, al ser un concepto de tipo funcional para la protección de esos derechos[44], la crítica se puede dejar de lado. Es decir, tomamos el contenido del derecho al anonimato como un aspecto necesario en el ámbito virtual donde de no existir habría un vacío que podría llegar a afectar a otros derechos ya consolidados.

Pero aún así, alguien podría preguntarse porque no proteger estos derechos en el ámbito informático por separado, en base a su resguardo esencial universalmente aceptado. Lessig nos da una luz en el tema *"¿De que manera los cambios en la tecnología deberían garantizar que los principios de un contexto anterior se presenten en otro nuevo? Es la misma pregunta que formulaba el Juez Brandeis en el caso de las escuchas telefónicas, una pregunta que el Tribunal Supremo responde continuamente, en multitud de contextos. Se trata, fundamentalmente de una cuestión acerca de la preservación de los principios cuando los contextos varían"*[45].

En el campo de nuestro estudio, el nuevo contexto es Internet. Donde hay una lucha de arquitecturas, es así como una arquitectura posibilitó el anonimato de las personas hay otra que se los pudo quitar. La pregunta entonces es: ¿qué es lo que hay que proteger? Hay que proteger aquellos bienes jurídicos que posibilitaban las mayores

[44] Nos referimos a la Privacidad, Inviolabilidad de las comunicaciones y autodeterminación informática.
[45] LESSIG, Lawrance, "El código y otras leyes...", Op. cit. p. 258

potencialidades de los usuarios en el ámbito de Internet. En palabras de Julio Cohen *"identifica un principio que una cierta arquitectura posibilitaba y que una nueva arquitectura amenaza para posteriormente defender el derecho afirmativo de proteger el principio original"*[46], y nuestro principio original es el anonimato. De ahí que lo reformulamos en el derecho al anonimato.

2.5 Expresión normativa del Derecho al Anonimato: Algunos ejemplos del derecho comparado.

Como analizamos anteriormente, en la práctica normativa será difícil encontrar un resguardo al derecho al anonimato como tal. Por el contrario, sí podemos verlo protegido a través del resguardo de bienes jurídicos tradicionales, como la inviolabilidad de las comunicaciones, la privacidad y la autodeterminación informática. Por lo mismo, un útil instrumento será el análisis de las Directivas Europeas 2000/31 y 2002/58 en cuanto tocan estos temas y son un referente a lo que podríamos tener a futuro en nuestro país.

La primera de las directivas mencionadas trata aspectos jurídicos de los servicios de la sociedad de la información, en particular en lo relativo al comercio electrónico. La segunda, relativa al tratamiento de los datos personales y la protección a la intimidad en el sector de las comunicaciones electrónicas. Cabe mencionar, que la Directiva 2000/31 ha sido implementada en España, en particular, en la Ley 34/2002 de servicios a la sociedad de la información y de comercio electrónico. Por ser España un referente para nuestra legislación, también consideramos prudente hacer algunas menciones a dicha ley. Hechas estas aclaraciones, veamos lo que se refiere al análisis en particular.

[46] Ibíd. p.259

- Derecho comparado: Directivas Unión Europea (2000/31), (2002/58) y Ley de Servicios de la Sociedad de la Información.

- Directivas Unión Europea (2000/31)

La primera mención que debemos hacer, es al considerando 15 de la mencionada Directiva. En ella se señala que:

"... los Estados miembros deben prohibir cualquier forma de interceptar o vigilar esas comunicaciones por parte de cualquier persona que no sea su remitente o su destinatario que esté legalmente autorizada"[47].

Claramente en esta situación vemos como se protege el bien jurídico mediante el resguardo a la inviolabilidad de las comunicaciones. La importancia de materias del comercio que requieren fundamental sigilo y secreto se debe imponer también en el ámbito de las comunicaciones electrónicas. En este sentido el anonimato se debe entender en la esfera de quienes realizan estas comunicaciones. De este modo, si bien no se reconoce el derecho como tal, si se atiende a su protección.

- **Directiva Unión Europea (2002/58)**

Lo primero que es interesante notar, es que ya en el considerando 9 se hace una referencia a la importancia del tratamiento en forma anónima de los datos personales. Es así como se señala que: *"Los Estados miembros, los proveedores y usuarios afectados y las instancias comunitarias competentes deben cooperar para el establecimiento y el desarrollo de las tecnologías pertinentes cuando sea necesario para aplicar las*

[47] Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). *Diario Oficial de las Comunidades Europeas.* 17 de Julio de 2000.

garantías previstas en la presente Directiva y teniendo especialmente en cuenta el objetivo de reducir al mínimo el tratamiento de los datos personales y de ***tratar la información de forma anónima*** *o mediante seudónimos cuando sea posible"*[48].

Es decir, se comprende la idea del anonimato como medio para proteger otras garantías que la Directiva propone. En este sentido, que la información sea tratada en forma anónima se traduce en el medio para que las instancias de las comunicaciones en el sector electrónico permitan a las personas salvaguardar los derechos fundamentales garantizados por los diversos Estados.

Ahora, en particular, el Artículo 6 es el que nos da la base para la protección del Derecho al Anonimato. En él se señala:

"Artículo 6

Datos de tráfico

1. Sin perjuicio de lo dispuesto en los apartados 2,3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o ***hacerse anónimos*** *cuando ya no sea necesario a los efectos de la transmisión de una comunicación."*

Así, para saber qué implica que se hagan anónimas tenemos que dar forma y consistencia a la existencia del derecho. Por ello es que pese a que en la expresión normativa se hagan referencias a los conceptos tradicionales del bien jurídico protegido tales como la privacidad o la inviolabilidad de las comunicaciones, el uso funcional del

[48] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de las Comunidades Europeas.* 31 Julio de 2002.

concepto del derecho al anonimato proporciona una herramienta de suma utilidad a efectos de resguardar a las personas, en este caso, en las comunicaciones.

- **Ley de Servicios de la Sociedad de la Información**

En la Ley de la Sociedad de la Información en su artículo 12 número 2 inciso tercero y cuarto se refiere a la importancia del correcto manejo del secreto las comunicaciones. En efecto, la citada disposición señala:

"En ningún caso, la obligación de retención de datos afectará al secreto de las comunicaciones.
Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley y ***deberán adoptar medidas de seguridad apropiadas para evitar*** *su pérdida o alteración y el* ***acceso no autorizado a los mismos****"*[49].

Se ve en este caso que el mencionado secreto, constituye un elemento fundamental a ser resguardado, y que sólo puede ser objeto de vulneración cuando los intereses superiores de la comunidad así lo aconsejen. De ahí que se hable del acceso no autorizado. Es así como además se confirma otro de los caracteres que puede rodear al derecho al anonimato: el bien común. En este caso, nos limitaremos a entender que el mismo está representado por lo que las leyes – y en última instancia los jueces – limitan como derechos superiores a los que se están vulnerando, v.gr.: derecho a la vida versus derecho a la vida privada, cuando se investiga un delito de homicidio y se registran comunicaciones.

[49] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (Versión consolidada no oficial). Artículo 12 n° 2, inciso 2º

La ley en cuestión, se enfoca , al resguardo de los secretos comerciales. Por lo mismo, se contemplan además exenciones de responsabilidad a la afectación de los bienes jurídicos. Así, se ve lo señalado en el artículo 15, que refleja lo que anteriormente expresábamos acerca de la protección del derecho más importante para el bien común.

3. Reseña Funcionamiento Internet: Del IPv4 al IPv6.

Para realizar una conexión a Internet es necesario establecer un vínculo entre dos puntos. Uno, el visible, es el punto de destino. Otro, el que a menudo se ignora, es el punto de origen de la conexión. El punto de origen de una conexión a Internet es la dirección IP.

Internet es una red integrada por cientos de miles de computadores. Estos computadores podemos, con fines explicativos, clasificarlos en dos tipos: servidores o usuarios**.** Un servidor es un computador que contiene información que puede ser consultada por usuarios. Por el contrario, un usuario es un computador que no está presentando información, sino que la va buscando. Todos los ordenadores de Internet, ya sean servidores o clientes, tienen que estar identificados de alguna forma. Y para ello se utiliza la dirección IP: cuatro números del 0 al 256 separados entre sí por un punto; por ejemplo, 185.47.814.2.

Internet es una red y, como toda red, ha de trabajar con un determinado protocolo de transmisión de datos, que indica cómo se efectúa la transferencia de información entre los computadores de la red. El protocolo utilizado por Internet se llama TCP/IP (Transmisión Control Protocol / Internet Protocol).

La dirección IP es la información mínima que proporciona cualquier usuario al conectarse a Internet. Una información mínima que puede llevar inscritos algunos datos más, como son el país o la organización de origen. Así, equivalen a las “huellas” que

dejan los usuarios que según dicha posición hacen imposible la existencia de un Derecho al Anonimato. A modo de ejemplo estas huellas alimentan los contadores de visitas puestos en una página Web y que sirven para elaborar todo tipo de estadísticas[50].

En tanto, los proveedores de Internet son compañías que han creado una conexión directa y permanente a Internet, ofreciendo la posibilidad de entrar en la red a través de ellos. Es decir, conectando con un proveedor se accede a todos los recursos de Internet.

Las direcciones IP pueden ser fijas o dinámicas. Una dirección IP fija (también llamada estática) es aquella que no cambia con el tiempo, permanece inalterable al reconectarse. Una vez asignada será la misma en cada conexión. Una dirección IP dinámica es aquella que es asignada mediante un servidor y que tiene una duración máxima determinada. Las IP dinámicas cambian cada vez que el usuario se reconecta.

El TCP/IP se compone de dos partes principales. La primera (TCP) es la parte de Protocolo de Control de Transmisión (*Transmission Control Protocol*) y la segunda parte (IP) es el Protocolo de Internet, un conjunto de reglas que gobiernan la forma en que viajan los datos de una maquina a otra a través de la red. La arquitectura para comunicar redes que usa los protocolos TCP/IP implica que todas las redes que intercambiarán información deben estar conectadas con equipos de procesamiento de información que son denominados compuertas. Tal arquitectura reconoce como iguales a todas las redes a conectar[51].

La versión actual del Protocolo Internet, IPv4, viene utilizándose desde hace más de 20 años. Cuando se diseñó en los años setenta no podía preverse el enorme

[50] MAYANS I PLANELLS, Joan, 2000, "Anonimato: el tesoro del internauta". Fuente Original: Revista iWorld (Octubre, 2000), pp. 52-59. Disponible en el ARCHIVO del Observatorio para la CiberSociedad en http://www.cibersociedad.net/archivo/articulo.php?art=28, última visita 2 de Junio 2005.
[51] VERCELLI, Ariel, La conquista silenciosa del Ciberespacio, http://www.arielvercelli.org/ , Marzo 2004, Buenos Aires, Argentina, p.103.

crecimiento de Internet. A modo de ejemplo, el nacimiento de la web sobrevino bastantes años después. Los diseñadores de Internet decidieron utilizar solamente 32 bits para representar las direcciones IPv4. Estos 32 bits permiten la utilización de 232 de direcciones IPv4 (un cifra alrededor de 4 000 millones).

El desarrollo exponencial que ha tenido Internet trae como consecuencia la escasez de direcciones IP. El que no se disponga de suficientes IP implica que las aplicaciones se vean obligadas a trabajar con mecanismos de direccionamiento de sitios locales. Se hace el símil con la situación que se vivía en los primeros días de la telefonía, cuando para realizar una llamada era necesario comunicarse con una operadora. Estos mecanismos limitan la funcionalidad en los extremos de Internet y reducen su rendimiento. El tipo de comunicación que se produce es del tipo cliente servidor, y el bajo rendimiento ocurre cuando un dispositivo externo desea establecer una conexión con el usuario, que es el tipo de comunicación entre pares.

Los nuevos servicios en Internet generan mayores exigencias técnicas. Dentro de los nuevos servicios se encuentran la televisión digital, telefonía IP, Mensajería universal, Chat de voz, PDA/Teléfonos móviles Wifi, entre otros. Estas nuevas prestaciones para su buen funcionamiento requerirán conectividad permanente con direcciones de IP exclusivas. Estar siempre conectados, dejará de ser una idea. Es por ello que surge una nueva versión del protocolo TCP/IP, el IPv6 que está compuesta por 8 segmentos de 2 bytes cada uno, que suman un total de 128 bits, a diferencia del anterior protocolo que sumaba 32 bits.[52] El nuevo protocolo Internet facilitará las posibilidades de conexión a la red mediante equipos terminales múltiples, como celulares, computadores personales u otros, mediante infraestructuras inalámbricas o por cable. Así, a modo de ejemplo, la transmisión más rápida de grandes cantidades de datos para varios destinatarios en video conferencia en línea.

[52] El cambio de la protocolo Internet es un ejemplo de cómo el diseño del código evoluciona. Finalmente es el código quien define el ciberespacio. Ver capítulo 4.1 Análisis crítico a la existencia de ser anónimo en la red.

La ventaja con respecto a la dirección IPv4 es en cuanto a su capacidad de direccionamiento. Tiene una capacidad de alrededor de 670 mil billones de direcciones por milímetro cuadrado de la superficie de la tierra.

Bajo un contexto de un espacio de direcciones IP amplio, implicará que toda una gama de nuevos servicios y aplicaciones de Internet sea posible. Los progresos esperados en las comunicaciones junto al uso de nuevos servicios multimedia interactivos a través de banda ancha son elementos que permiten vaticinar que se progresará paulatinamente hacia el IPv6.

El IPv4 no desaparecerá de la noche a la mañana. La actual implantación del IPv6 se realiza en paralelo al IPv4.

Junto a las ventajas que plantea el IPv6 se presentan una serie de dificultades. Una de ellas es la posibilidad de la integración de un número de identificación único en la dirección IP de los terminales de los equipos de telecomunicaciones. Es más, con la amplitud de direcciones IP, todo equipo electrónico será susceptible de poseer una. Se multiplicarán las terminales conectadas a la red[53].

Las desventajas que se avizoran son:

1- El uso de un identificador único constituye un riesgo de elaboración de perfiles de las personas, a través del conjunto de las actividades que realiza en la red.

2- El nuevo protocolo permite conexiones estables, manteniendo la misma dirección, incluso cuando un equipo se desconecta de la red. En este caso, la seguridad y la

[53] A los ya clásicos teléfonos celulares y computadores personales se sumarán los dispositivos electrónicos que controlan los aparatos domésticos de calefacción o alarmas por ejemplo.

confidencialidad son problemáticas, dado que existe un peligro de identificación de los datos relativos a la localización.[54]

Ante estos riesgos es que concordamos con la opinión que plantea que la dirección IP es un dato personal. Así lo afirma la Unión Europea, a través del grupo de protección de datos personales[55]. El derecho fundamental a la intimidad y a la protección de los datos está consagrado en la Carta de derechos fundamentales de la UE y desarrollado en las directivas comunitarias sobre protección de datos. *"El considerando 26 de la Directiva 95/46, los datos se considerarán personales en cuanto se pueda establecer un vínculo con la identidad del interesado (en este caso, el usuario de la dirección IP) mediante medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona. En el caso de las direcciones IP, el proveedor de servicios de Internet siempre puede establecer un vínculo entre la identidad del usuario y las direcciones IP, tal como podrían hacer otros, utilizando por ejemplo registros disponibles de direcciones IP asignadas o utilizando otros medios técnicos"*[56].

Para lograr un equilibrio entre los derechos fundamentales de los usuarios y los intereses de los distintos participantes se debe aplicar el principio de la proporcionalidad tratando el menor número de datos posible para la realización de la comunicación. Las consecuencias de este principio se traducen en que "*las aplicaciones y diseño de nuevos aparatos de comunicaciones deben respetar la privacidad"* [57]. En la conexión de telecomunicaciones, "*los proveedores de red o de acceso deben ofrecer a cualquier*

[54] Dictamen 2/2002 del grupo de protección de de datos personales la Unión Europea , sobre el uso de identificadores únicos en los equipos terminales de telecomunicaciones : Ejemplo del IPv6. Adoptado el 30 de Mayo 2002.
[55] Órgano asesor sobre protección de datos e intimidad establecido por la Directiva 95/46CE del Parlamento Europeo y del Consejo 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, Diario Oficial de 23 Noviembre 1995.
[56] Dictamen 2/2002, op. cit. p.3.
[57] Ibíd. p.3.

usuario la opción de utilizar la red o de acceder a los servicios de forma anónima o mediante un seudónimo"[58]. Un ejemplo para lograr ese anonimato en las comunicaciones por Internet es el cambio periódico de las direcciones IP de una persona.

4. Problemas que origina ser anónimo en la Red.

El ser anónimo en Internet genera una serie de problemas. En una primera índole está el hecho que el anonimato implica una dificultad para la detección de los autores de los delitos que se cometen en los medios informáticos. Toda investigación penal tiene en la mira la investigación de los hechos constitutivos del delito y principalmente la detección de los autores, para ello resulta imprescindible contar con medidas que permitan la identificación de los sujetos que participan de los hechos punibles, y con la existencia del anonimato en la red, esta situación se hace más difícil. También está el hecho que el anonimato junto con ser una garantía para la libertad de expresión, es considerado un fomento para la difusión de contenidos difamatorios o injuriosos.

El debate en torno a infracciones al Derecho al Honor y a la propia imagen, se desarrolla en torno a reclamaciones contra proveedores de servicios de Internet por mensajes con contenido difamatorio o injurioso, o también la publicación de fotografías íntimas. El determinar al autor de la difusión de esos contenidos es complejo, ya que es identificable la máquina a través de la cual se difundió el contenido, pero no así con seguridad al autor del mismo. Situación similar se ha señalado que ocurre con la difusión de material protegido por las leyes de propiedad intelectual. La situación de anonimato fomentaría la ocurrencia fraudes a través de Internet. Lo claro es que el proceso de identificación de los responsables en la red, se torna, en principio, más dificultoso que en el espacio real.

[58] Ibíd. p.4.

Estas situaciones que pueden aparecer como negativas deben ser contrastadas con las positivas, en "*la red, cualquier persona puede publicar su material para todos los demás, independiente del lugar geográfico en que se encuentre. Las redes posibilitan la publicación de cualquier texto sin pasar por criterios de selección, por procesos de edición o por la determinación de responsabilidades"*[59]. El anonimato concebido como una imperfección de la Red por Lessig implica que "*no existe una manera sencilla ni de conocer la identidad de quienes están conectados ni de clasificar los datos, tampoco existe una manera sencilla de condicionar el acceso a los datos dependiendo de la identidad de quien desea obtenerlos. En una palabra, no existe una manera eficiente de zonificar al ciberespacio"*[60].

-Análisis crítico a la existencia de ser anónimo en la Red.

Corresponde ahora hacerse cargo de las críticas que se configuran sobre el Derecho al Anonimato. Una primera línea de críticas dice relación con cuestionar su existencia en Internet desde un carácter que llamaremos fáctico técnico. Hay quienes señalan que el Anonimato no es más que un mito, algo irrealizable toda vez que la comunicación a la red se basa en protocolos IP. El usuario desde que ingresa a la red va dejando huellas y esas huellas revelan información. Así en un contexto social y cultural, en él la población se siente clasificada y controlada, como si de una ficha dentro de una inmensa base de datos se tratara, el anonimato parece ser la solución pero no dejaría de ser un sueño tan apetecible como irrealizable.

Siguiendo con esta línea técnica hay que referirse a lo que Manuel Castells llama genéricamente como tecnologías de control, en donde incluye lo que son tecnologías de control, vigilancia e investigación[61]. La diferencia muchas veces entre estas tecnologías

[59] LESSIG, Lawrence, "El código y otras leyes...", Op cit. p.45.
[60] Ibíd. p.64.
[61] CASTELLS, Manuel, "La galaxia...", op. cit. p.195-209.

puede resultar muy tenue, así a modo de ejemplo las tecnologías de vigilancia sirven a las tecnologías de investigación y trazar los límites de cada uno puede resultar ser una tarea muy difícil. De esta manera las tecnologías de control incluyen el uso de contraseñas, cookies y procesos de autentificación.

Las tecnologías de vigilancia son aquellas que interceptan mensajes y colocan marcadores que permiten rastrear los flujos de comunicación desde un determinado ordenador y controlar la actividad de la máquina. Las tecnologías de investigación, por su parte, atañen a la elaboración de bases de datos mediante los resultados de la vigilancia y la acumulación de información.

El modelo básico de cookies es un archivo que es introducido en el ordenador del usuario por algunos sitios Web que éste visita. Estas contienen información sobre las visitas previas que el usuario ha realizado a aquella página y esta información puede ser más o menos abundante, dependiendo del uso que se le quiera dar. De este modo, puede consistir en un sencillo código invisible asignado a cada visitante para contabilizar cuántos usuarios vuelven a la página después de haberla descubierto, únicamente con fines de control y cómputo interno.[62] Se pueden presentar como invasivos de la privacidad del usuario pero también como necesarios para facilitar las comunicaciones, en sí no tienen un carácter ilegítimo, pero el argumento de la crítica se basa en que lo claro es que se dejan huellas del navegante en la red, y ello impide o limita enormemente el anonimato.

Contra esta crítica que hemos denominado de orden fáctico técnico exponemos nuestro desacuerdo, pese a la fuerza de los argumentos. Una cosa es dejar huellas en el camino de Internet, lo que técnicamente sucede cada vez que uno navega, y otra que esas

[62]Manuel Castells al conceptuar las cookies dice que son marcadores digitales que los sitios web colocan automáticamente en los discos duros de los ordenadores que se conectan a ellos. Una vez que se han insertado las cookie, todos los movimientos on line realizados desde dicho ordenador son grabados automáticamente por el servidor del sitio web que los colocó.

huellas sean pesquisables y que configuren un identidad virtual. La circunstancia de dejar huellas por Internet deriva de su uso, el ejercicio de un Derecho no puede constituir a la vez su propio límite. El límite del Derecho al Anonimato no es absoluto, y va ceder en circunstancias que se protejan otros bienes jurídicos como es el caso de la persecución de delitos, pero el que se dejen huellas no impide el Anonimato de los usuarios.

La importancia del uso de estos dispositivos es tal que ha sido recogido normativamente por la directiva 2002/58 de la Unión Europea, Directiva sobre Privacidad y Comunicaciones electrónicas. Así este es un argumento a nuestro favor, en cuanto si bien se pueden dejar huellas en la navegación hay interés en respetar el que se mantenga el anonimato de los usuarios. En el considerando 25 de dicha Directiva prevé que los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal una cookie o dispositivo semejante. A tal fin, también se deberá facilitar a los usuarios información clara y precisa sobre la finalidad y la función de estas.[63]

Una segunda línea de críticas, que proviene principalmente del ámbito jurídico, tiene relación con que la naturaleza de la red viene determinada por sus arquitecturas[64]. Éstas son expresadas en una suerte de "código", término acuñado por Lessig con el que designa a las aplicaciones de hardware y software que funcionan sobre los protocolos TCP/IP. Podemos ampliar la acepción que Lessig confiere al término, y esto comprendería a todo el conjunto de elementos integrantes de la configuración técnica de las comunicaciones en el ciberespacio. De este modo, por ejemplo, las cookies son elementos del Código.

---

[63] En los casos en que estos dispositivos, (*cookies*), tengan un propósito legítimo, como el de facilitar el suministro de servicios de la sociedad de la información, debe autorizarse su uso a condición de que se facilite a los usuarios información clara y precisa al respecto, de conformidad con la Directiva 95/46/CE, para garantizar que los usuarios están al corriente de la información que se introduce en el equipo terminal que están utilizando. Los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal una *cookie* o dispositivo semejante.

[64] LESSIG, Lawrence, "El código y otras leyes...", op cit. p. 67.

El usuario no se percata que obedece algunas reglas *sui generis*, un código o regulación *técnica* de Internet. Como dice Lessig *no es la naturaleza quien determina el ciberespacio, sino el código: «el hardware* y el software, que hacen del ciberespacio lo que es, regulan el ciberespacio tal como es»[65]. Lo que se configura progresivamente es una arquitectura panóptica que posibilita el control perfecto. Lessig señala que la causa de esto es la arquitectura de Internet que se presenta como elástica unido a los intereses del comercio y del gobierno.

En este sentido, Manuel Castells disiente de la postura normativa que toma Lessig, pero señala que debe tomarse como punto de partida de cualquier análisis, la transformación de la libertad y la privacidad en Internet es consecuencia directa de su comercialización. En sus palabras "*la necesidad de asegurar e identificar la comunicación para poder ganar dinero gracias a la red y la necesidad de proteger los derechos de propiedad intelectual, han derivado en el desarrollo de nuevas arquitecturas de software que posibilitan el control"*[66].

Subyace la idea de que el ciudadano no quede como sujeto Anónimo. La regulación de conductas en el ciberespacio, la ley en este caso, la arquitectura es el código y el código regula la conducta en términos que determina cuáles conductas pueden llevar a cabo los individuos en el ciberespacio y cuáles no, con esto se le quita el sustrato al Derecho al Anonimato. A modo preliminar, como contra crítica a la postura de Lessig, señalaremos que el problema no es tanto del Código sino de la habilidad de la sociedad para modificar el Código, resistirse a él o imponerlo[67]. Lo cual nos lleva a plantearnos de qué manera se resiste al código o se logra modificar éste. En el concepto de Lessig el anonimato es provocado por la imperfección del Código y como el Código tiene una tendencia a perfeccionarse es allí donde se originan los problemas. En opinión de Manuel Castells "*técnicamente, Internet es una arquitectura de libertad. Socialmente,*

[65] Ibíd. p. 207.
[66] CASTELLS, Manuel, "La galaxia..." op. cit. p. 198.
[67] Ibíd. p. 209.

sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los transgresores, lo cual implica la definición de la trasgresión y la existencia de técnicas de vigilancia eficaces"[68].

El enfoque que da Manuel Castells no es tanto desde la perspectiva del Código, sino desde la del usuario y sus relaciones sociales. Señala que tal como existen tecnologías que posibilitan la vigilancia y el control, a su vez existen tecnologías que garantizan la libertad, sin embargo no todo es tecnología en la defensa de la libertad. *"En realidad, lo más importante no es la tecnología sino la capacidad de los ciudadanos para afirmar su derecho a la libre expresión y a la privacidad de la comunicación (...) En último término, es en la conciencia de los ciudadanos y en su capacidad de influenciar sobre las instituciones de la sociedad, a través de los medios de comunicación y del propio Internet, en donde reside el fiel de la balanza entre la red en libertad y la libertad en la red."*[69]. En cambio, Lessig en todo momento se refiere a la idea de modificar el Código, *"la manera más efectiva de regular el comportamiento en el ciberespacio será a través de la regulación de código – regulación directa ya sea del código del ciberespacio en sí mismo, o de las instituciones (escritores de códigos) que producen el código"*[70].

Al comparar el mundo real con el mundo virtual Lessig hace hincapié en que determinados grados de libertad que se dan en el mundo real son productos de un alto costo de control, más que de una adecuada configuración normativa protectora de la

---

[68] CASTELLS, Manuel, "Internet, Libertad y Sociedad : Una perspectiva Analítica" , Lección inaugural del curso académico 2001-2002 de la UOC (Universitat Oberta de Catalunya). http://www.uoc.edu/web/esp/launiversidad/inaugural01/intro_conc.html# . Última visita 2 de Junio 2005. Disponible también en revistapolis, Revista On-Line de la Universidad Bolivariana Volumen 1 Número 4, año 2003, http://www.revistapolis.cl/4/cas.pdf , última visita 2 de Junio 2005.

[69] Ibíd. p. 21.

[70] LESSIG, Lawrence, "La ley del caballo", http://www.derecho.udp.cl/site/apuntes%5Cint%5Cla_ley_del_caballo_llessig.PDF, Traducido por Iñigo de la Maza Gazmuri y Ximena Escobar Pozo. Programa Derecho y Tecnologías de la Información. Fundación Fernando Fueyo Laneri, Facultad de Derecho Universidad Diego Portales, p. 13. Última visita 2 Junio 2005.

libertad. Cuando los costos se reducen, hay que tomar una decisión, o se permite la erosión o se establecen límites. Por ello se debe dotar al ciberespacio de una arquitectura que asegure el anonimato, en la mayor medida posible. Si el Código va a monitorizar lo que hago, al menos no debería saber que soy "yo" el sujeto sometido a monitorización. El planteamiento, se resume en lo siguiente: *"el derecho es vulnerable a la soberanía competitiva del código. Los escritores del código pueden diseñar códigos que desplacen los valores comprendidos en el derecho. Si estimamos que los valores del derecho deben sobrevivir, el derecho debería responder a esto"*[71].

Capítulo II.

Internet: Regulación y Prestadores de Servicios.

1. Regulación en la Red.

Las ventajas de Internet como medio de comunicación tales como la rapidez, bajos costos e interconectividad traen aparejados otros problemas como el control de contenidos, la normativa aplicable y en general, problemas asociados con su regulación. Así, en un primer aspecto se puede considerar la regulación de quienes prestan el servicio de Internet. En un segundo plano de quienes lo usan. Si bien en ambos casos lo que se puede realizar es menor en consideración a los sistemas de regulación tradicionales en otras esferas de la sociedad, es en el campo de los prestadores de servicios donde se puede pensar en algún mayor control. En el caso de los usuarios este control es mucho menor, pero no imposible. Sí pudiese ser visto como algo a largo plazo, ya que en este caso, la regulación pasa más bien por la educación que es la base fundamental de lo que luego denominaremos autorregulación.

[71] Ibíd. p.41.

Para introducirnos al tema, es conveniente hacer algunas referencias al porqué debemos regular la red. Al respecto es Jijena Leiva, quien nos da algunas ideas. De este modo él señala algunos ámbitos que implican mayor debate sobre temas de regulación jurídica en la red. Algunos de ellos son:

"Los contenidos – lícitos o ilícitos – de la información que navega por la red, lo que ha motivado intentos de censura de algunos gobiernos;

- La forma en que se ve afectada la propiedad intelectual de los autores de bienes ahora inmateriales o digitalizados que están en Internet, en particular de libros y programas computacionales que se usan o "bajan" sin pagar las licencias respectivas , y en general de todos los contenidos distribuidos en línea;

- Las particularidades de los contratos de acceso a Internet que se celebran con los llamados "proveedores de servicios de Internet" -en especial de conectividad- o "ISP" , sean nacionales o internacionales, gratuitos u onerosos; y,

- La protección de la privacidad de las personas, en especial del anonimato de los usuarios o "navegantes del ciberespacio ", de manera tal que accedan a sitios Web sin temor a que queden registrados sus movimientos y a que se acumule información sobre su persona que luego pueda ser usada indebidamente"[72].

Así el primer problema se plantea con los contenidos que circulan por la red. En estos casos se puede tratar tanto de contenidos lícitos como ilícitos. En los primeros, su regulación no se liga al manejo ilícito de los contenidos. Por el contrario, se trata de elementos que a todas luces pertenecen al área de lo permitido tanto en Internet como en

[72] JIJENA LEIVA, Renato. *Informe legal: sobre la improcedencia de censurar legalmente los contenidos de Internet. Análisis del Boletín N°2395-19.* REDI: Revista Electrónica de Derecho Informático. Número 15. Sección III.

cualquier otro medio de comunicación. Lo que aquí sucede es el tratamiento que se le da a estos contenidos lícitos. De este modo, los datos personales de una persona, imágenes, videos, o cualquier información que le pertenezca no producen un ilícito en contenido. El ilícito se puede ver por la conducta y no por el contenido. Es el caso de datos que se hagan de conocimiento público sin el consentimiento de la persona o bajo su reprobación.

Luego, en el ámbito de los contenidos ilícitos, la regulación va directamente relacionada con el resguardo penal de las comunicaciones. La red puede materializarse como el puente mediante el cual los delitos comunes pueden encontrar un canal de transferencia para sus cometidos. La regulación de los contenidos ilícitos, ira directamente asociada a la sanción penal que se tenga de los ilícitos cometidos mediante la red. Pero, por otro lado, la persecución penal de los hechos que revistan caracteres de delitos trae consigo el monitoreo de las acciones que puedan aparecer como propicias para el cometidos de los mismos. Ello tanto en el ambiente físico como el virtual. De ahí que la regulación de los contenidos ilícitos además, plantea el problema de la regulación mediante monitoreo de las comunicaciones y contenidos de la red. Es ahí donde se cae en el complejo problema de decidir cómo hacerlo, cuanto hacerlo, y según algunas posturas más liberales, si es que se debe hacer.

En el caso de la protección de la propiedad intelectual mediante la regulación de los contenidos de la red el problema reside básicamente en los mecanismos para atentar contra los programas y materiales protegidos por la ley de propiedad intelectual. En este sentido, se puede argumentar en contra de los sostenedores de páginas web que pongan a disposición de usuarios los medios necesarios para hacerse de programas, músicas, videos y otros sin pagar los respectivos derechos de propiedad intelectual. Pero el conflicto se pone aun más difícil de regular al momento de entrar en el ámbito de los programas de conexión directa entre personas. En este caso, surge la pregunta de cómo regular lo que por estos programas circula. Ya no se trata de contenidos alojados en

determinados servidores, sino de materiales que se comparten directamente desde el computador de un usuario a otro.

Ahora, en el caso de los proveedores de servicios a Internet, el conflicto reside en como controlar la información que éstos manejan respecto a los usuarios. En este sentido vale la pena mencionar la problemática que se produce al analizar los diferentes registros de conexión que los proveedores de servicios puedan tener. Muchas veces estos contratos de servicios de conexión no reportan las prácticas que las empresas manejan en el ámbito de facturación y registros de tráfico. Otra veces, estas se encuentran explícitas, mas no lo suficientemente claras para que el usuario promedio pueda entenderlas.

Finalmente, la regulación de la red tiene un punto de inflexión en el ámbito de la protección del anonimato en la red. Es común que los distintos sitios web utilicen medidas tecnológicas para poder analizar la procedencia de sus visitas y las características de las mismas.

De este modo, vemos como la regulación en la red habla de diversos aspectos a ser considerados en función de hacer respetar el resguardo de las garantías fundamentales de los usuarios. Tanto en el ámbito civil, como en el penal. Desde la perspectiva del interés de la sociedad hasta el interés individual. En este sentido, la regulación se ha visto ya desde distintos prismas. Por un lado, desde la acción estatal y la regulación de los ordenamientos jurídicos nacionales en conjunto o aisladamente. Por otro, desde la regulación de los mismos usuarios que llevan a comprometer procesos de largo plazo donde se involucran los diversos aspectos de protección a los derechos que la sociedad les garantiza. Estos son los puntos que desarrollaremos a continuación.

1.1 Regulación Estatal en una Red mundial.

Nos señala Jijena Leiva que *"...en la práctica no es tan simple aplicar el derecho tradicional en el ambiente del ciberespacio o de las redes digitales, que transmiten información de diversa naturaleza a alta velocidad y que permiten interconectar al mundo completo....Hay que entender que para abordar la problemática de la red, imaginaria -y geográficamente- debemos situarnos en el lugar físico o en el país donde esté instalado un servidor computacional que provea dichos contenidos (cosa que tecnológicamente puede no ser tan fácil de determinar). No hay que atender al Estado o país en que estén ubicados los usuarios-navegantes de la red, porque éstos, telemáticamente y a través del ciberespacio lo que hacen es llegar hasta o acceder a ese determinado servidor y a las páginas con diversos contenidos (los menos son los ilícitos) que en él se mantienen, porque ellos lo desean así y porque libremente han optado por acceder a dichos sitios, acción virtual que tecnológicamente se materializa porque varios ISP o proveedores de conectividad lo posibilitan mundialmente"*[73].

Por ello que el problema de la regulación estatal dice relación con el imperio efectivo que ha de tenerse junto a las posibilidades de sanciones reales frente a la infracción. Es decir, nos encontramos ante un fenómeno global de alcances mundiales versus la acción local de entes centralizados. De este modo "*Internet –una red telemática pública y abierta- descansa en su "no regulación" o "desregulación local", lo que implica que no se puede censurar desde un Estado determinado una realidad virtual que -normativamente y en teoría- sólo podría llegar a regularse mediante un tratado internacional, siempre y cuando existan criterios uniformes respecto a la forma de hacerlo, v.gr., respecto a la improcedencia de difundir contenidos pornográficos. Pero ocurre -es la realidad- que en países más liberales como Holanda la pornografía*

[73] *Ibíd.*

no es considerada ilegal, al menos no al nivel de países más conservadores como Chile"[74].

De ahí que en la regulación estatal, además del problema sobre el alcance de la jurisdicción, está el conflicto con las distintas definiciones que los diversos Estados dan a los tipos de bienes jurídicos que se resguardan. Sin embargo, estas consecuencias no implican que la regulación estatal sea un fin utópico. En primer lugar, debemos considerar que muchos delitos que se pueden cometer por medio de la red tienen una connotación de delitos universales. Así sucede con la pornografía infantil por ejemplo. En el campo de los derechos civiles, la vida privada y el resguardo de los datos sensibles, representan derechos definidos en cualquier régimen democrático actual.

Ahora bien, también debemos considerar las herramientas principales mediante las cuales la regulación se hará efectiva. Tradicionalmente esa regulación ha recaído sobre el control que los entes estatales tienen sobre los Prestadores de Servicios de Internet. Mediante esta normativa, el estado es capaz de definir responsabilidades en el caso de ciertos actos cometidos mediante la red. Es decir, se tiene control sobre el medio a través del cual los posibles ilícitos o lesiones a los bienes jurídicos protegidos se cometen. De este modo las regulaciones normalmente establecen causales de responsabilidad. Tanto en concordancia con las causales legales generales como en el cumplimiento de la legislación común aplicada a Internet. También se contemplan medidas aplicables en cuando las capacidades técnicas lo permitan y, en muchos casos, dando un margen de *razonabilidad* a los prestadores de servicios para que estos eliminen o controlen los contenidos de sus servidores en cuanto así lo estime el sentido común[75]. Por último los controles estatales también contemplan causales de eximición de la responsabilidad de los prestadores de servicios en cuanto se cumplan los requisitos establecidos. Ello con el fin de no cargar toda la responsabilidad en ellos, lo cual de una

[74] *Ibíd.*

[75] Es interesante notar como en estos casos se entremezcla la figura de la regulación estatal con la autorregulación que puedan ejercer los ISP, tema que será analizado más adelante.

u otra manera traería costos insospechados además de perjudicar la libertad y flexibilidad propia de Internet.

Como vemos, la regulación no es lejana a la realidad, pero sí debe contemplar los diversos aspectos que hemos mencionado. Es por ello que la acción estatal en la red, si bien es compleja, no es del todo ausente y, por el contrario, tiene, por el momento el rol principal dentro de los cauces en los cuales se lleva a cabo la regulación en Internet, desplazando por el momento al rol que pueda jugar la autorregulación. Algunos ejemplos de esta realidad las analizaremos en el apartado 6 de este capitulo mediante un análisis comparado. Pero primero realizaremos algunos comentarios sobre lo que se ha denominado la autorregulación.

1.2 Autorregulación.

Al hablar de autorregulación en la red, nos referimos a la posibilidad que sean los mismos actores de la Internet quienes pongan los controles en su uso. Ello con prescindencia del elemento normativo del poder estatal, total o parcialmente. En esta visión podemos encontrar básicamente dos actores. Por un lado lo que los propios Prestadores de Servicios de Internet, y por otro los usuarios en general. En el primer caso, la autorregulación se puede observar siguiendo la lógica del mercado como analizaremos a continuación. En el caso de los usuarios, la autorregulación va más bien por el lado de la educación.

Cuando hablamos de la autorregulación de los Prestadores de Servicios de Internet, lo primero que tenemos que tener claro es que estamos hablando de compañías de negocios. Por lo mismo, debemos recordar que como tales las compañías son neutrales moralmente. No obedecen a los mismos dictámenes que las personas naturales. Por el contrario, su capacidad de respuesta se lleva más bien por lo que dicte el ordenamiento legal o la lógica de mercado. En el caso de la autorregulación, por tanto,

se debe poner énfasis en el funcionamiento del mercado. ¿Cómo influye esta lógica en la autorregulación? Mientras las empresas que promueven la autorregulación obtengan algo beneficioso a cambio, habrá incentivos para que ésta se practique.

Núñez Errázuriz nos señala al respecto: *"Los argumentos en favor de la autorregulación se basan en el argumento de que las OAs* (Organizaciones Autorreguladas) *deben cuidar su reputación ante los consumidores; si la reputación es valiosa en una industria caracterizada por información asimétrica sobre calidad, entonces las Oas intentarán construir una reputación de proveer buena calidad. Esto se lograría primeramente, supervisando y monitoreando la calidad al interior de la OA, y en segundo lugar, informando a los consumidores sobre la calidad provista. Una investigación teórica de esta hipótesis requiere analizar cómo la reputación puede originarse y legitimarse ante los consumidores, y cómo ésta puede sostenerse en el tiempo. La reputación, a su vez, dependería de la estructura informativa específica disponible a los consumidores, la cual permitiría a los consumidores formarse expectativas sobre la calidad esperada. Las Oas podrían tener los incentivos apropiados bajo algunas estructuras informativas pero no en otras"*[76].

En el caso de los Prestadores de Servicios de Internet, esta reputación se construye mediante la calidad impuesta a favor de sus usuarios. En este sentido, el manejo de las políticas de privacidad y alojamiento de contenidos no mantendrán indiferentes a sus usuarios. Por supuesto, ello requiere de la adecuada información de parte de los ISP hacia sus usuarios. En este sentido, si las personas ven que las políticas de privacidad del Prestador al cual están accediendo respeta y conserva su derecho a la vida privada – a la sazón al anonimato si se acepta esta nomenclatura – la reputación del ISP crecerá entre sus usuarios con el consiguiente beneficio económico.

[76] NÚÑEZ ERRÁZURIZ , Javier, "La Autorregulación como Concepto Regulatorio." Documento de Trabajo Nº171, Departamento de Economía, Universidad de Chile, Santiago, 2000, p.11.

Lo mismo sucede con otras áreas de autorregulación. Veamos el caso de Microsoft y el cierre de sus salas de chat en MSN. La medida sin duda evitaba posibles problemas legales que pudiesen surgir a raíz del aumento de la pornografía infantil y spam a través de dicho medio. Pero fue una medida unilateral de Microsoft, una medida de autorregulación efectivamente. Al respecto la explicación de los ejecutivos de MSN Microsoft se dio profusamente en los medios: *"Queremos mejorar la protección de la juventud en Internet", dijo un portavoz. "Hay cada vez más personas que dan mal uso a los foros de chateo. Algunos usuarios, por ejemplo, usan las direcciones de e- mail de los jóvenes con intenciones dudosas. Por ejemplo, se distribuyen fotos pornográficas o direcciones de páginas web con contenidos pornográficos. "La pornografía infantil es un motivo para cerrar los chats", dijo el portavoz.* ***"Con esto, nuestros usuarios están mejor protegidos del spam****", explicó Judy Gibbons, vicepresidenta de MSN"*[77].

El énfasis que se pone en que los usuarios estarán mejor protegidos del spam con esta medida no es casual. Ello representa a MSN Microsoft como una mejor empresa, preocupada de sus usuarios y sobre todo del bien social. ¿Cabe preguntarse cuantos padres habrán contratado MSN más seguros después de la noticia? Así es como funciona la autorregulación. En el caso de los datos personales, se aplica la misma lógica. Para una empresa es de suma importancia saber de antemano cómo y bajo qué normativa interna los ISP tratarán sus contenidos privados. Por ello bajo este prisma creemos que la autorregulación es posible.

Veamos ahora el caso de la autorregulación en los usuarios. Una de las propuestas más interesantes en este ámbito son las ideas de autorregulación mediante asociaciones que representen a los usuarios. Ya sea a iniciativas de entes estatales o como organizaciones de consumidores. Jijena Leiva señala sobre el particular: *"También deben considerarse como una opción jurídica viable las modalidades de autorregulación. Por su propio peso e importancia el desarrollo y los conflictos*

[77] Diario La Tercera. 24 de Septiembre de 2003.

jurídicos en Internet pueden traducirse en el surgimiento de normativas que, impulsadas por algún país u organismo internacional, tengan acogida y sean aceptadas mundialmente por los usuarios de la red. Así ha ocurrido con la reglamentación desarrollada por la IANA y la ICANN en relación a la asignación de direcciones virtuales o de los nombres de dominio"[78].

Es decir, el orden natural de la red parece haber sido acomodado mediante la necesidad de establecer regulaciones que vayan más allá de las medidas impositivas de los gobiernos centrales. Dado que Internet se vislumbra como descentralizado y autónomo se ve que más allá de establecer ordenamientos estructurados a seguir lo que se debe hacer son labores de coordinación para permitir la autorregulación. De este modo, *"algo cercano a la autorregulación es la existencia de verdaderas "entidades de coordinación". Efectivamente Internet no es controlada directamente por ninguna empresa u organización específica, pero, al decir de la Red Universitaria Nacional -REUNA- en el seno de entidades internacionales se han ido generando políticas para permitir un desarrollo sustentable y la interoperabilidad entre redes regionales y nacionales, analizar la implementación de nuevos estándares, y evitar el crecimiento explosivo, por ejemplo, del flujo de datos en la red o del número de usuarios. Se trata de una coordinación importante y necesaria, que ha sido asumida por entidades como la Internet Society, que es la organización internacional para la cooperación y coordinación global de Internet, sus tecnologías de interconexión y sus aplicaciones"*[79].

La autorregulación resulta positiva toda vez que Internet es un fenómeno en constante construcción. *"Es positiva la regulación de la Red pues se deben fijar las "reglas de juego" pero, no debemos olvidar que la normativa que regule este fenómeno debe estar en permanente construcción porque la propia realidad de Internet así lo requiere. Es obvio que es necesaria una regulación mínima y flexible pero, al mismo*

[78] Jijena Leiva, Op. cit. Sección III.
[79] Ibíd.

tiempo, que garantice la libertad de la Red y, le aporte el grado de confianza que demanda la sociedad"[80].

Por último, cabe mencionar la autorregulación quizás más lejana pero no por ello desechable: la del usuario individual. Ello se debe a la propia regulación de los contenidos de los que se dispone en la red. Tanto en su emisión como en su recepción. Ya hemos mencionado como uno de los problemas que presenta la red en relación a la protección del derecho al anonimato son los que se generan con la recopilación de datos personales mediante las denominadas *cookies.* Si los usuarios toman conocimiento y conciencia de lo que a través de estos mecanismos se puede realizar protegerán en mayor medida la fuga de datos que se está produciendo en la actualidad. Lo mismo sucede con la relación que los usuarios puedan tener con los Prestadores de Servicios de Internet. Si existe educación y conciencia la autorregulación podrá verse aplicada en la exigencia recíproca de cuidado en el manejo de datos sensibles hasta los datos de facturación. El usuario debe conocer los registros que los Prestadores de Servicios mantienen, usan y la medida en la cual éstos pueden o no hacerse públicos.

Cabe terminar este apartado señalando algunos interesantes comentarios que – aplicados al tema que acabamos de analizar con las características del caso – pueden abrir una interesante opción en el dilema de la regulación y autorregulación. Señala Núñez Errázuriz: "*La supuesta ineficiencia implícita en la combinación de regulación pública y la autorregulación no debe ser materia de creencia o suposición. Por el contrario, se propone que ésta debe ser una hipótesis a ser investigada formalmente. Al margen de los obvios costos de duplicación, existen al menos tres posibles consideraciones que hacer respecto de las implicaciones de superponer regulación pública y la regulación privada (autorregulación). Primero, la regulación pública, ceteris paribus, conduciría al descubrimiento de fraude que de otro modo no sería*

[80] ORTEGA, Alfonso "El Derecho a la Protección de Datos de carácter personal en Internet", Memorias del X Congreso Iberoamericano de Derecho e Informática, Lom ediciones 2004 p.235.

descubierto y permanecería impune. Segundo, la regulación pública puede cambiar el comportamiento de los miembros de la OA (Organización Autorregulada)*, quienes finalmente determinan la calidad. Tercero, la regulación paralela también puede alterar los incentivos hacia la vigilancia que las OAs enfrentan. La conjetura principal y la motivación fundamental para esta línea de argumentación es que la regulación paralela permitiría aprovechar la ventaja informacional de las OAs, pero al mismo tiempo generando los incentivos adecuados para monitorear la calidad y hacer pública cualquier evidencia de fraude, incentivos que presumiblemente las OAs no regulada voluntariamente podrían no poseer sin regulación paralela"*[81].

1.3 Proyectos de Ley sobre Regulación de Internet.

Un breve análisis de los proyectos de ley que regulan Internet nos permiten visualizar como se aborda el fenómeno de la regulación de la red por parte de los legisladores.

1-Boletín Nº 2395-19 sobre regulación de Internet. Este proyecto de ley contiene 5 artículos, que consideramos relevante el primero. Dicho artículo señala: *"El que difunda o propale a través de los sistemas, redes y procedimientos de Internet, o de otros servicios de igual naturaleza, informaciones, contenidos o noticias contrarias a la moral, el orden público, o las buenas costumbres será sancionado con una multa de 15 Unidades Tributarias Mensuales.*

Igual sanción se aplicará a quienes usen dolosamente tales servicios y redes con el propósito de incitar al odio y la discriminación contra grupo de personas en razón de su raza, nacionalidad, sexo o religión; y a las que utilicen esos servicios o redes para difundir pornografía o efectuar una apología de la violencia."

[81] Núñez Errázuriz, *op. cit.* p. 13.

El error básico de esta norma es asimilar Internet a un medio de comunicación social y no percatarse que en Internet no hay un editor responsable[82]. Dicha norma propuesta además adolecería de inconstitucionalidad[83]. El proyecto de ley fue archivado en abril 2002 por la Cámara de Diputados.

2- Boletín Nº 2512-07 sobre comunicaciones electrónicas: Ingresado por moción de los diputados Alberto Espina y Patricio Walker el 13 de junio de 2000. El proyecto fue archivado y sólo se recogieron algunas normas en la ley de firma electrónica publicada en el Diario Oficial con fecha 12 de Abril de 2002.

Este proyecto intentó regular una gran cantidad de temáticas que tenían relación con las nuevas tecnologías. Entre los tópicos que intentó regular se encuentran la seguridad jurídica en las transacciones electrónicas, la Privacidad, Nombres de Dominio, Propiedad Intelectual, los contenidos (lo que se conoce como contenidos ilícitos y nocivos). De todas las disposiciones del el proyecto creemos necesario hacer referencia a lo concerniente a los contenidos.

El inciso 6º del artículo 19 del proyecto de ley sobre comunicaciones electrónicas señala que "*los prestadores de servicios, "**no tendrán obligación de supervisar los datos que transmitan, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas**; sin perjuicio de cualquier*

[82] Sobre este punto JIJENA LEIVA, Renato, "Informe Legal: sobre improcedencia de censurar legalmente los contenidos de Internet. Análisis del Boletín Nº 2395-19" en Revista Electrónica de Derecho Informático. Número 15 Octubre 1999.
http://premium.vlex.com/doctrina/REDI_Revista_Electronica_Derecho_Informatico/Informe_legal_improcedencia_censurar_legalmente_contenidos_Internet_Analisis_Boletin_N%B02395-19/2100-107405,01.html , (última visita 2 de Junio 2005).

[83] Sobre la inconstitucionalidad de la norma propuesta ALVAREZ VALENZUELA, Daniel. "La regulación de Internet en Chile", en Revista Chilena de Derecho Informático Nº 3, Diciembre 2003, p. 181-191. El autor señala que la moción parlamentaria propone restringir el ejercicio del derecho a la libertad de expresión no dando cumplimiento a ninguno de los requisitos que nuestro ordenamiento constitucional exige, esto es que 1-Que la ley debe perseguir uno de los objetivos mencionados en el artículo 13 Nº 2 de la Convención Americana de Derechos Humanos 2-Necesariedad para la consecución de dichos objetivos. 3- Proporcionales al fin buscado.

*actividad de supervisión, selectiva y transitoria**, que las autoridades competentes soliciten a tenor de lo dispuesto en la legislación vigente, cuando resulte necesario para garantizar la seguridad del Estado, la defensa, la seguridad pública y para prevenir, investigar, detectar y perseguir delitos y abusos sancionados por la ley*.

Sin perjuicio de lo señalado en el inciso anterior, los prestadores de servicios de acceso a la red de comunicaciones, sólo podrán prestar sus servicios si ofrecen sistemas de filtros de contenido, que permitan a sus usuarios bloquear o discriminar por categorías la información que reciban a través del respectivo proveedor". (El subrayado y negritas es nuestro)[84].

---

[84] El Artículo 19º del proyecto de ley sobre comunicaciones electrónicas Boletín Nº 2512-07 en forma integra dice: "*Cualquier persona podrá publicar en o por medio de un sistema informático toda clase de información, en cualquier forma, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas libertades, en conformidad a la ley.*

El prestador de servicios de transmisión por una red de comunicaciones de datos facilitados por el destinatario del servicio o de servicios de acceso a la red de comunicaciones, no será responsable de los datos transmitidos, salvo que:

a) el prestador de servicios haya originado él mismo la transmisión,

b) el prestador de servicios haya seleccionado al destinatario de la transmisión,

c) el prestador de servicios haya seleccionado o modificado los datos transmitidos.

Los servicios de transmisión y acceso antes referidos incluyen el almacenamiento automático, provisional y temporal de datos transmitidos, siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión.

En todo caso, el prestador de servicios de transmisión por una red de comunicaciones de datos facilitados por el destinatario del servicio o de servicios de acceso a la red de comunicaciones, no será responsable del almacenamiento automático, provisional y temporal de esa información, efectuada con el solo propósito de hacer más eficiente su retransmisión a otros destinatarios del servicio que la hayan solicitado, siempre que:

a) el prestador del servicio no modifique la información,

b) el prestador del servicio respete las condiciones de acceso a la información,

c) el prestador del servicio respete las normas relativas a actualización de la información, indicadas de forma coherente con las normas de la industria,

d) el prestador del servicio no interfiera con el uso legítimo de tecnología, coherente con las normas de la industria, que se utilice con el fin de obtener datos sobre utilización de la información, y

e) el prestador del servicio actúe con prontitud para retirar la información o bloquear el acceso a ella, en cuanto tenga conocimiento efectivo que la información ha sido retirada del lugar de la red en que se encontraba inicialmente, se ha hecho imposible acceder a dicha información, o la autoridad competente ha ordenado retirar esta información o ha prohibido que se acceda a ella.

Asimismo, el prestador de servicios de almacenamiento de datos proporcionados por el destinatario del servicio, no será responsable de los datos almacenados a petición del destinatario, siempre que:

a) el prestador de servicios no tenga realmente conocimiento que la actividad es ilícita y,

b) en cuanto tenga conocimiento de su ilicitud, el prestador de servicios actúe con prontitud para retirar los datos o bloquear el acceso a ellos.

Otro aspecto de este proyecto de ley esta en la imposición de una obligación a los ISP de acceso de prestar servicios de filtros de contenido para poder prestar sus servicios. Dicha obligación esta imbuida en cierta fe en que los sistemas de filtro son la solución ante los contenidos ilícitos en la red, sin embargo los sistemas de filtro aún son imperfectos.

3- Boletín Nº 3004-17 sobre Responsabilidad en Internet: Este proyecto fue ingresado a tramitación legislativa el 18 de julio de 2002. El proyecto se encuentra en el Segundo trámite Constitucional. Dentro de las normas de dicha moción que es necesario analizar se encuentra el Artículo 1° que señala:

"Cualquier persona podrá publicar en o por medio de un sistema de información toda clase de datos, en cualquier forma, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas libertades, en conformidad a la ley".

Este artículo no es más que una declaración de principios. Se le critica su carácter confuso, en cuanto a que la expresión sistema de información es muy amplia, y podría incluirse a los sistemas de información de redes privadas.[85] El legislador sólo pensó en sistema de información haciéndolo sinónimo con la red abierta pública que es Internet situación que es errónea.

En todo caso, los prestadores de servicios referidos en los incisos precedentes, no tendrán obligación de supervisar los datos que transmitan, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas; sin perjuicio de cualquier actividad de supervisión, selectiva y transitoria, que las autoridades competentes soliciten a tenor de lo dispuesto en la legislación vigente, cuando resulte necesario para garantizar la seguridad del Estado, la defensa, la seguridad pública y para prevenir, investigar, detectar y perseguir delitos y abusos sancionados por la ley.

Sin perjuicio de lo señalado en el inciso anterior, los prestadores de servicios de acceso a la red de comunicaciones, sólo podrán prestar sus servicios si ofrecen sistemas de filtros de contenido, que permitan a sus usuarios bloquear o discriminar por categorías la información que reciban a través del respectivo proveedor. Estos sistemas deberán incorporarse obligatoriamente a los servicios de acceso a redes informáticas que se provean a los establecimientos educacionales, sean públicos o privados. Las características técnicas mínimas que deberán cumplir los filtros serán establecidas mediante Decreto Supremo, suscrito conjuntamente por el Ministerio de Transportes y Telecomunicaciones y el Ministerio de Educación.

[85] ALVAREZ VALENZUELA, Daniel, Op. cit. p.190.

Otro artículo relevante es el artículo 4º que señala:

"Los prestadores de servicios de transmisión, acceso y almacenamiento referidos en los artículos anteriores no tendrán obligación de supervisar los datos que transmitan, ni la obligación de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, sin perjuicio de cualquier actividad de supervisión, específica y transitoria, que las autoridades judiciales soliciten para prevenir, investigar, detectar y perseguir delitos y abusos en conformidad a la ley".

La gran importancia de dicho artículo está dada por cuanto los Isp no se les faculta para actuar como censores de la información que por ellos transita o se aloja.

Luego de revisar someramente algunas de las disposiciones de estos proyectos de ley es menester señalar que se nota una evolución en el conocimiento de las características del funcionamiento de Internet. Es así que se pasa de un proyecto de ley que no tiene claridad conceptual y que en la práctica es irrealizable, a proyectos con mayor elaboración y mayor precisión.

En estas normas se trasluce el derecho al anonimato. No hay una declaración formal del derecho, pero hay principios que protegen al usuario de Internet. Uno de ellos es la libertad de expresión de los usuarios de Internet. El otro es que los Isp no tienen obligación de indagar quien es el sujeto que hay al otro lado de la pantalla, sólo tienen el deber de colaborar con la justicia. Existe implícita una libertad de navegación anónima, en el sentido que los Isp no están obligados a supervisar los datos que transitan en la red.

2. Libertad en Internet.

Cuando nos planteamos los problemas que se pueden dar en la regulación de los derechos público y privado en Internet, partimos desde una de las premisas que distinguen a este medio de comunicación. Ello es la libertad que otorga la red en comparación a los otros medios. Algo ya esbozamos sobre las limitaciones que aun así existen en las regulación de los números IP. Sin embargo, la libertad y anonimato de la red no se ven limitadas en otros aspectos de las comunicaciones cibernéticas.

En esta materia los defensores de las libertades privadas gozan de elementos a su favor. En primer lugar, las características propias de la red, como internacionalidad, descentralización, etc.… a las cuales ya algo nos hemos referido. En segundo lugar, la propia tecnología que da alimento y sustento a la red. Ella es muchas veces más rápidamente manejada por los usuarios que por los mismos reguladores de la red. A cada salvaguarda que existe se da una posibilidad de romperla. La regulación estricta da paso a mayores posibilidades de intromisión autónoma. De ahí que la libertad pareciere estar ganando la batalla en los campos bélicos del ciberespacio.

Pero no todo está dicho en materia de regulación. Tanto en la persecución de ilícitos penales como en la protección de datos de carácter privado la regulación puede provenir de diversas fuentes. Muchas veces de los mismos usuarios a los cuales se pretende regular: "De aquí la inclinación preferente por sustituir la regulación pública por la autorregulación de los agentes que intervienen, a través de los cuales se lleva a cabo el tráfico de la comunicación en Internet"[86]. ¿Pero como podríamos hablar de

[86] MUÑOZ MACHADO, Santiago, "La Regulación de la Red: Poder y Derecho en Internet". Editorial Taurus, Madrid 2000. p. 157.

autorregulación en los contenidos de comunicaciones privadas? En materia europea han sido varios los intentos por fomentar la autorregulación[87].

Muchas veces, incluso no existe conciencia del bien jurídico de la privacidad. Materias conocidas por terceros muchas veces ni siquiera son elementos de la preocupación del usuario. Sólo llegan a ser de su conocimiento cuando por infortunados hechos, el usuario se entera de que hay otros que saben mucho de él mismo. Momento en que la mayoría de las veces es demasiado tarde en el mundo de Internet.

Es por ello que muchas veces la libertad propia de la red puede tener grandes posibilidades para resguardar la privacidad en Internet. Incluso una acción coactiva de los entes reguladores puede generar más reacciones adversas que las que se pretenden evitar. La acción mancomunada de la sociedad civil y el gobierno, es esencial en cualquier regulación. La misma idea se encierra en un elemento que comentábamos anteriormente. Asociaciones de consumidores fuertes y con un marco de legitimidad que les permitan actuar frente al poderoso manejo de información que poseen los ISP. Quizás suene un poco lejano a la realidad nacional, pero no por ello menos deseable.

Lo mismo sucede con la información de los derechos del usuario. La autorregulación y la protección de las libertades que se puedan realizar de la red, no contarán con suficiente aceptación si está no es seguida de cerca por los sujetos a quienes se pretende proteger. Nos señala Muñoz Machado: *"En cuanto a los derechos del interesado, además de la expresión de su voluntad, que acaba de indicarse, los más notables son los de información, acceso, oposición y rectificación. El de información le debe permitir obtener del responsable del tratamiento o su representante todos los datos relativos a quien es el responsable del tratamiento, los fines del mismo y los*

[87] Así el recomendar seguir acciones de filtros, educación y elección de contenidos en la red. Dentro de estos aspectos, que mejor ejemplo de un campo fértil a la autorregulación y la protección de los mismos usuarios, que en materia de las *cookies.*

destinatarios. En cuanto al acceso, se debe consentir a los interesados el ejercicio del derecho a obtener libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos, la confirmación de que existe el tratamiento de datos, los que, en concreto, son objeto de tratamiento, y el origen de los mismos. Por lo que concierne al derecho de oposición, se trata de que pueda el interesado, en determinados casos, evitar por razones legítimas e impedir el tratamiento de datos que le conciernan. Y, en fin, la rectificación se reconoce siempre al interesado, junto con el derecho de supresión o el bloqueo, de los datos de cuyo tratamiento no se ajuste a las disposiciones de la directiva"[88].

Si bien en nuestro país la regulación en esta materia por parte del ordenamiento jurídico no es exhaustiva aún, sí podemos pensar en usar los elementos que se poseen en la actualidad para determinar y hacer cumplir estos derechos. Nos referimos a elementos tan simples como las garantías constitucionales consagradas en la carta magna, como a los diversos tratados internacionales de protección a las libertades individuales que hoy están vigentes en Chile.

De este modo se puede empezar a crear una conciencia del ciberespacio. En la actualidad, la violación de un derecho en otros medios de comunicación es asumido por la población como un ilícito. Al leer cualquier materia que nos lleve a plantear el cuestionamiento de la intervención telefónica o de correspondencia, el rechazo es espontáneo. Lograr la misma razón en materias electrónicas, parece ser un paso no sólo útil a la adecuada defensa de sus intereses, sino también necesario.

[88] MUÑOZ MACHADO, Santiago, "La Regulación ..." , op.cit. p. 184.

-Libertad de Expresión.

Un análisis específico merece el planteamiento que realiza Lessig en torno a la libertad de expresión en el ciberespacio. Para ello se debe recordar que la regulación incluye no sólo aquélla que se realiza mediante normas jurídicas, sino que, la regulación es el resultado de la interacción de cuatro elementos, donde la norma jurídica sólo es uno de sus elementos que interactúa con los demás. Los elementos que están presentes en la regulación son la ley (que debe ser entendida en un sentido lato como toda norma jurídica), el mercado, la arquitectura y las normas sociales. La importancia de distinguir estos diferentes elementos está en el hecho de establecer que la libertad de expresión está protegida por algo más que la ley en el ciberespacio. En el *ciberespacio "la libertad de expresión viene limitada por algo más que el Estado y, de la misma manera, viene protegida por algo más que el Estado"*[89].

El mercado favorece la libertad de expresión de los sujetos en el ciberespacio, esto por cuanto las restricciones que impone el mercado en el ciberespacio son mínimas comparadas con las del mundo real. Sólo basta traer a colación los costos que implicaría para un sujeto editar un libro o acceder a un medio de comunicación masivo, frente al costo que implica acceder al ciberespacio y exponer sus ideas, junto al hecho de la multitud de gente a la cual puede llegar su mensaje.

Las normas sociales no interfieren con la libertad de expresión, como lo hacen en el mundo real, el repudio social a una determinada expresión en el ciberespacio sólo se ve enfrentada a las críticas ejerciendo el mismo derecho a expresarse libremente, *"en el ciberespacio se da una mayor tolerancia hacia las personas que disienten cuando se sabe o se cree saber, o se supone que quien las expresa vive a KM. de uno"*[90].

[89] LESSIG, Lawrance, "El código y otras leyes...", op. cit. p. 303.
[90]LESSIG, Lawrance, "El código y otras leyes....", op. cit. p. 307. También al respecto de este tema los cuestionamientos que realiza Muñoz Machado en cuanto a que debido a las características de la red (principalmente el tema de la llamada multiubicación) disminuyen la capacidad de replica de los sujetos.

Dentro de todos estos elementos que se han señalado es la arquitectura la que favorece la libertad de expresión en la red en mayor medida, esto por cuanto "*el relativo anonimato, la distribución descentralizada, los múltiples puntos de acceso, la no necesaria vinculación geográfica, los sistemas poco eficaces de identificación de contenidos, las herramientas de encriptación, todas estas características y consecuencias del protocolo Internet dificultan el control de la expresión en el ciberespacio*[91].

Uno podría pensar que, si el real protector de la libertad de expresión en el ciberespacio es la arquitectura, deberíamos quedarnos tranquilos, porque en definitiva el elemento tecnológico (la arquitectura) nos garantiza, mejor que la ley, el derecho a expresarnos. Es un error considerar a la tecnología (arquitectura) como algo dado de carácter inmodificable, prácticamente, como algo del mundo natural al cual debe el hombre acomodarse como sea. Si hay algo en el mundo que no pertenece al entorno natural es la tecnología. Considerarla como parte de este último y asumir que no puede modificarse, implica una pérdida de poder por parte de la comunidad[92]. Para explicar este punto se hace necesario un ejemplo. El ser humano ante un suceso de la naturaleza debe acostumbrarse o acomodarse. Ante un día de lluvia se usa un paragua o se moja, no es posible cambiar la lluvia por sol. La tecnología puede ser cambiada, y si alguna restringe el anonimato no debe ser aceptada como algo incuestionable.

Ante la exposición de la Harvard Law Review de mayo de 1999, Vol. 112 que expresa que en el ámbito virtual todos estamos en igualdad de condiciones, los personajes públicos y los privados, sobre todo porque cualquiera puede aclarar y replicar inmediatamente, poniendo en circulación la verdad y deshaciendo la difamación con tanta prontitud y extensión como se ha difundido. Ante esta afirmación tan alentadora, Muñoz Machado se pone en el caso de las difamaciones y señala "*que se exagera un poco la capacidad de replica en el ciberespacio, no tiene en cuenta que es necesario acceder al mismo foro en el que la difamación se ha producido y hacerlo rápidamente."* MUÑOZ MACHADO, Santiago "La Regulación de la Red. Poder y Derecho en Internet", Editorial Taurus. Madrid, 2002. p. 173-174.

[91] LESSIG, Lawrance, "El código y otras leyes...", op. cit. p.307.

[92] En terminología de Castells el poder de la sociedad radica en su capacidad para modificar el código, resistirse a él o imponerlo. Castells, Manuel, "La Galaxia...", op. cit. p. 209.

Es lógico que no todos tengamos las capacidades técnicas o cognitivas para entender el funcionamiento de la red, pero no por ello se debe aceptar a priori a las nuevas arquitecturas, más aún cuando estas tienden a cambiar producto de la interacción con los otros elementos como son el mercado y la ley. Es aquí en donde entran a jugar las interacciones de los elementos antes mencionados, y esa interacción se ve manifestada en que, a través de la ley, es posible modificar directa o indirectamente a la arquitectura[93]. Se podría sostener que, para preservar la libertad, la red debe ser un campo que este libre de toda regulación. No es esa la idea que se defiende en estas líneas, regulación no es sinónimo de control, "*las arquitecturas ya están siendo reestructuradas con el fin de volver a regular lo que la arquitectura del espacio real hacía regulable anteriormente. La red ya está pasando de ser libre a estar controlada"*[94].

Un ejemplo nítido de lo anterior se da con la DMCA[95] calificada como Orwelliana, ejemplo de cómo una ley interactúa con las arquitecturas de Internet en el campo de la propiedad intelectual. La DMCA es una respuesta de tipo legal a la incertidumbre que generó aquella problemática en el mundo del ciberespacio. Junto a esta repuesta de carácter legal está la respuesta de carácter tecnológico, que es la creación de nuevas tecnologías de protección de la propiedad intelectual, estas controlan la distribución y copia del material protegido por las leyes. Así "*la DMCA era una creación legal con el objetivo de respaldar la protección de este código diseñado para proteger materiales con copyright. Era, podríamos decir, código legal que tenía el*

[93] LESSIG insiste en la relación que existe entre la arquitectura y la libertad que posibilita, y como la ley participa en la construcción de dicha arquitectura. Lessig, Lawrence, "El código y otras leyes ....", op. cit. p. 308.
[94] Ibíd. p.308-309.
[95] Digital Millenium Copyright Act. Análisis de la normativa en JOSE ERNESTO FERNANDEZ PINÓS [et al.]; Fermín Morales Prats [y] Óscar Morales García coordinadores. "Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet", Editorial Aranzadi, 2002. También análisis en "Las consecuencias no deseadas: Cinco años bajo la Digital Millenium Copyright Act". Electronic Frontier Fundation, Traducción desde el inglés de Alberto Cerda Silva, Coordinador Académico del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, revisada por Patrick Humphreys Neumann, Abogado. http://www.eff.org/IP/FTAA/5_Anos_de_la_DMCA,_eff_3.pdf (última visita 20 enero 2004).

objetivo de afianzar código informático que en sí mismo tenía el objetivo de apoyar el código legal copyright."[96] , la libertad de expresión se ve controlada en el ciberespacio por cuanto la DMCA hace que difundir información que proporcione los medios para violar las medidas tecnológicas de protección sea constitutivo de delito[97]. Esto trae como consecuencia una pérdida de debate académico, que se deje de investigar y difundir el conocimiento científico[98].

En el ámbito europeo, de acuerdo a Pérez Luño, la libertad de expresión en la red sólo puede verse limitada en virtud de la defensa de derechos ajenos, en concreto de los menores y la dignidad de las personas condicionada a tres exigencias acumulativas:

1) *Prohibición de arbitrariedad*, lo que implica que cada restricción deba estar prevista por la ley;

2) *Necesidad social* imperiosa de garantizar valores y derechos de las sociedades democráticas;

3) *Legitimidad de objetivos,* enumerados de forma limitada y entre los que la defensa de la moralidad y la salud públicas se estiman particularmente adecuados para proteger a los menores y la dignidad humana.

---

[96] LESSIG, Lawrence, "Cultura libre cómo los grandes medios están usando la Tecnología y las leyes para encerrar la cultura y controlar la creatividad". Traducción ANTONIO CÓRDOBA con una licencia de Creative Commons. http://cyber.law.harvard.edu/blogs/gems/ion/Culturalibre.pdf. p. 179.

[97] Los ejemplos que señala Lessig donde producto de la unión de lo que es la ley y la arquitectura se ve restringida la libertad de expresión, son por una parte la publicación en Internet de una ponencia académica que mostraba los fallos de un sistema para la distribución de música en Internet desarrollado por SDMI (iniciativa para música digital segura). Dicha ponencia se enmarca dentro de lo que es un debate académico, no podría ser constitutivo de delito. El otro ejemplo dado son páginas web de fanáticos de mascotas virtuales en donde informaban como "enseñarle" trucos para bailar a las mascotas, esos trucos violarían las medidas tecnológicas de protección con lo cual también serían un delito. De ahí cierta ironía al concluir que uno puede enseñarle a bailar a su perro real, pero no puede enseñarle a bailar a su perro robot. Más sobre diferentes casos producto de la DMCA en Electronic Frontier Fundation, "Las consecuencias no deseadas", Op. cit p. 16 http://www.eff.org/IP/FTAA/5_Anos_de_la_DMCA,_eff_3.pdf , última visita 15 de Junio 2005.

[98] Las consecuencias no deseadas: Cinco años bajo la Digital Millenium. op. cit, p. 4.

Es fácil inferir los problemas que pueden derivarse de la precisión de lo que, en cada caso, deba considerarse como "necesario" para legitimar una medida legal restrictiva y que persiga un "objetivo legítimo". No basta para ello que tal medida resulte "útil" o "razonable". El carácter legítimo de la medida sólo puede probarse tras un profundo examen de su eficacia en relación con el grado de injerencia que implica. Este análisis constituye una *prueba de proporcionalidad* de las medidas restrictivas[99].

No hay que dejarse engañar con el hecho de que en un determinado momento la libertad de expresión se vea beneficiada por una determinada arquitectura, por cuanto ella puede cambiar. Al final se trata de defender ciertos principios, "*tenemos un principio no sólo porque es ley, sino porque es verdaderamente una gran idea. Una tradición de libertad de expresión fuertemente protegida es probable que dé pie a una amplia gama de discurso crítico. Este discurso es probable, a su vez, que mejore los sistemas o la gente o las ideas criticadas"*[100].

3. Prestadores de Servicio de Internet.

Uno de los problemas que plantea la investigación tiene relación con el funcionamiento de los sistemas de Prestadores de Servicios de Internet o ISP, por sus siglas en inglés. Aún cuando la regulación jurídica en cuanto a los bienes protegidos sea extensa, ésta puede quedar rápidamente obsoleta si no se entiende cómo funcionan los ISP. Si bien existen prácticas necesarias que los proveedores deben cumplir, hay otras que son posibles tecnológicamente, pero van más allá de lo que al derecho le concierne o incluso lo que al derecho le interesa proteger.

[99] PERÉZ LUÑO, Antonio-Enrique, "Impactos sociales y Jurídicos de Internet", Argumentos de Razón Técnica, Revista española de Ciencia, Tecnología y Sociedad, y Filosofía de la Tecnología, http://www.argumentos.us.es/numero1/bluno.htm , (última visita 3 de Junio 2005).
[100] LESSIG, Lawrance, " Cultura libre...", Op. cit. p.178.

En primer lugar, es necesario conocer su modelo de funcionamiento técnico. No es materia de esta investigación hacer un estudio acabado sobre el tema, pero con algunas nociones básicas podremos encontrar la base suficiente para poder entrar a discutir las materias propiamente jurídicas. En segundo lugar, hemos de plantear las prácticas necesarias que deben realizar los ISP. Así, por ejemplo, la inclusión y registros de tiempos e información para efectos de facturación. Por último, las prácticas y usos que según estos estándares se dan en relación a los intereses jurídicos en juego. Tanto del punto de vista de la tutela estatal sobre los derechos cautelados para la sociedad toda, como del punto de vista de los derechos del individuo.

En cuanto al funcionamiento técnico es interesante tomar en cuenta el gran desarrollo que han tenido las redes de telecomunicaciones en los últimos años. Ello hace cuestionarse la proyección a futuro de los actuales sistemas de comunicación. De este modo, si bien hoy podemos manejar la información que es posible recabar mediante el sistema de funcionamiento de los ISP, tal vez en un año o menos esa información quede obsoleta. De ahí a que la protección jurídica si bien debe acotarse a los medios técnicos mediante los cuales se puede manejar la información – y por ello su buen o mal uso - no debe quedar restringida a elementos definitorios que lo limiten en el tiempo. Una buena forma de realizar esto, será entregando los elementos técnicos de regulación a la potestad normativa reglamentaria, de rápida adecuación en el tiempo y variable por naturaleza[101].

Ahora bien, volviendo a los elementos técnicos propiamente tal, lo primero que hay que tener presente es que la Internet otorga elementos únicos de privacidad y anonimato que en parte le hacen única. Pero ello no es absoluto. Tanto en el mundo electrónico como en el real, hay ciertos elementos que permiten identificarnos, y como tal, hacen que poseamos características únicas que pueden ser de interés propio o ajeno.

[101] Es un punto de interesante discusión que da para otra investigación, pero que en está al menos se tocará tangencialmente en las conclusiones.

La identificación de Internet se asocia con el número IP. Ella es la que "*determina en cada momento a una máquina en Internet o a un conjunto de máquinas constituidas en una red*"[102]. En otras palabras la dirección IP es lo que permite identificar a los ISP qué máquina y en qué momentos se está conectando al sistema. Por ende, quien es el titular que ellos registran de esa maquina y en una primera instancia la titularidad de la persona que hace uso de aquellos servicios.

Mediante este sistema los ISP poseen los elementos técnicos para almacenar toda la información necesaria sobre los tiempos de conexión, lugar desde el cual se realiza e incluso las materias a las cuales la conexión se refiere. Vale decir, bajo los parámetros estrictamente técnicos, los ISP tienen el poder de conocer toda nuestra intimidad por la red desde el momento en que empezamos nuestra conexión hasta que apagamos la misma.

Entonces, muchas veces el problema reside en quién y cómo maneja esta información. En la mayoría de los casos al contratar un servicio de comunicaciones por Internet, los usuarios no tienen la opción de determinar convencionalmente los posibles usos y prácticas que las empresas darán a estos servicios. Por ello queda al ordenamiento jurídico esta tarea.

Pero hay prácticas que se manifiestan como necesarias al momento de definir los usos de los ISP. Así por ejemplo los datos necesarios a la facturación. Ellos deben guardarse con el objeto de conocer una adecuada información de carácter comercial que permita a las empresas el funcionamiento de sus servicios de cobro. Ello está generalmente aceptado y regulado, pero también hay que considerar que aún por lícita y

[102] LOPEZ MELGAREJO, Antonio. "Investigación Criminal y Proceso Penal: Las Directrices de la Propuesta del Consejo de Europa sobre Cyber-Crime y de la Directiva del Comercio electrónico". En Revista Derecho Procesal y Penal, número 8, Ed. Aranzadi, Navarra, 2002. p. 250

necesaria que parezca esta actividad implica peligros sobre el manejo de estas bases de datos.

En otro aspecto, estos datos se mantienen en reserva absoluta (o al menos así lo dicta la teoría) sobre el acceso que pueden tener a ellos las personas en el ámbito privado. Pero no sucede lo propio en el aspecto público. El manejo de los datos de IP (número IP y tiempo de conexión) puede llegar a ser conocido mediante la investigación en un proceso, normalmente mediante la intervención del Ministerio Público. Este problema ya se dio en España y en la actualidad es un asunto que entrará a la discusión en nuestro país. Así por ejemplo durante una época "continuaba siendo frecuente que no se facilitaran dichos datos entretanto no mediara habilitación judicial, lo que motivo la consulta 1/1999 (RCL 2000, 876), sobre Tratamiento Automatizado de Datos Personales en el Ámbito de las Telecomunicaciones, por la que el Fiscal del Estado, en fecha 22 de enero de 1999, estableció la necesidad de mediación judicial, viniendo a motivar dicha necesidad en la interpretación de que el artículo 18 de la Constitución Española de las comunicaciones, sino el propio hecho de que una persona se comunique, y por lo tanto dé los datos asociados a cada comunicación. En la actualidad, en consecuencia, cualquier solicitud dirigida a los ISP en demanda de datos, no ya de carácter personal, sino meramente técnicos, se realiza previa habilitación judicial"[103].

Cabe agregar que las prácticas necesarias de los ISP deben quedar reguladas no sólo por el ordenamiento jurídico, sino también por una efectiva acción fiscalizadora por parte de los organismos del Estado encargados de la supervigilancia de estas empresas. En Chile esta misión queda a cargo de la Subsecretaria de Telecomunicaciones. Una cuenta que no debería dejar de lado el poder que eventualmente pueden ejercer organizaciones de consumidores bien establecidas, paso que en nuestro país aun parece ser un poco incipiente.

[103] Ibíd. p.. 252

Por último, las prácticas de los ISP quedarán en gran medida determinadas por los usos y permisos que dé el ordenamiento jurídico al sistema. Por citar algún ejemplo, cabe recordar la nueva legislación sobre pedofilía, que da un plazo de 6 meses en que deben mantener esos registros. Pero la práctica usual es que éstos se mantengan sobre el tiempo de conexión y el IP. No sobre los datos que se ingresan o reciben en ese tiempo de conexión. Dicho de otro modo, permisión para saber cuándo se conecta una persona y durante qué tiempo, pero no qué hace durante ese tiempo. Estas materias entran delicadamente en lo más íntimo de los derechos de las personas, tocando directamente un bien protegido como es la inviolabilidad de las comunicaciones.

3.1 Tipos de Prestadores de Servicios.

La normativa de la Subtel[104] distingue dos tipos de prestadores de servicios de Internet. Uno es el **ISP o proveedor de acceso a Internet** que lo define como la persona natural o jurídica que presta el servicio de acceso a Internet, de conformidad a la ley y su normativa complementaria. El segundo es el p**roveedor de contenido** que es la persona natural o jurídica que pone a disposición de los usuarios contenidos y/o aplicaciones en Internet a través de medios propios o de terceros[105].

Al respecto hay que hacer mención a lo que señala DELPIAZO al tratar sobre los nuevos roles en la sociedad de la sociedad de la Información: distingue entre lo que son los servicios en la sociedad de la información de lo que son los servicios del ciberespacio. Dentro de estos últimos es que se encuentran los actores objeto de nuestro estudio. Estos llamados servicios del Ciberespacio son producto de "*la potenciación de la Informática por las Telecomunicaciones, lo que podía aparecer como una simple relación entre un emisor de un mensaje de datos y un destinatario del mismo aparece*

[104] Subsecretaria de Telecomunicaciones, dependiente del Ministerio de Transportes y Telecomunicaciones.
[105] Resolución exenta Nº 1.483 que Fija procedimiento y plazo para establecer y aceptar conexiones entre ISP.

mediatizada en el espacio telemático por la intervención de una pluralidad de sujetos que la facilitan, la hacen posible o la determinan, según los casos. Entre ellos, cabe distinguir entre los proveedores de servicios propiamente dichos, y los proveedores de contenidos"[106].

Es posible distinguir entre los prestadores de servicios los siguientes tipos:

-Proveedores de acceso y transmisión.

- Prestadores que realizan copia temporal de los datos.
- Proveedores de Alojamiento.
- Proveedores de motores de búsqueda o enlaces[107].

En la práctica, la delimitación de los distintos proveedores de servicios se hace difícil, por cuanto, es común que los proveedores de acceso faciliten otros servicios de Internet a sus clientes, como la posibilidad de almacenaje u otros servicios adicionales.

La distinción que se realiza de estos prestadores de servicios se hace en virtud de sus funciones. El TLC con EE.UU. en el capítulo 17 se realiza una clasificación de los proveedores de servicios de Internet atendiendo a su función. Así, la norma en cuestión limita la responsabilidad de los proveedores de Servicios de Internet a las funciones de: 1-Transmisión, enrutamiento o suministro de conexiones para el material sin modificar su contenido. 2- almacenamiento temporal (caching) llevado a cabo mediante un proceso automático. 3- Almacenamiento a petición de un usuario de material que se aloja en un sistema o red controlada u operada por o para el proveedor, incluidos correos electrónicos y sus archivos adjuntos almacenados en el servidor del proveedor, páginas Web alojadas en el servidor del proveedor. 4- Referir o vincular a los usuarios a un sitio

[106] DELPIAZO, Carlos, *"El nuevo Derecho en la Sociedad de la Información",* Edición Digital Actas del X CONGRESO IBEROAMERICANO DE INFORMÁTICA Y DERECHO, Santiago, Chile, Septiembre 2004, pp. 20-25.

[107] La Ley Española sobre sociedad de la información realiza esta clasificación de acuerdo a las 4 funciones.

en línea mediante la utilización de herramientas de búsqueda de información, incluidos hipervínculos y directorios.

De todas estas clasificaciones de los prestadores de servicios de Internet, nos interesa la de los prestadores de acceso y transmisión, conceptuado como aquel que permite la conexión lógica y entrada a la red. Esto porque el usuario de Internet el primer contacto que tiene con el ciberespacio es a través de su Isp de acceso, su anonimato dependerá en gran medida de su desempeño. Si no se le exige preservar el anonimato al primer actor que interactúa con el usuario, se torna más complicado exigirlo a los demás actores. Así que cuando nos refiramos a prestadores de servicio debe entenderse a los proveedores de acceso.

3.2 Obligaciones de Prestadores de Servicio de Internet con sus usuarios.

Una empresa o un individuo pueden desempeñar distintos papeles en Internet y, por lo tanto, ejecutar simultáneamente distintas operaciones de tratamiento de datos (por ejemplo, registro de conexiones en calidad de operador de telecomunicaciones o almacenamiento de sitios web visitados en calidad de *proveedor de servicios de Internet*), con todo lo que esto implica en la aplicación de principios sobre privacidad.

El proveedor de acceso a Internet proporciona, generalmente sobre la base de un contrato, una conexión TCP/IP a personas que utilicen un *módem* o un adaptador de terminal. En este caso, el abonado recibirá una dirección IP válida durante la conexión que probablemente cambiará la próxima vez que se conecte y se denomina dirección IP dinámica. Si se trata de una línea *ADSL* (conexión a través de una línea de suscripción asimétrica digital) o de cable de vídeo, la dirección IP será normalmente estática, pues dichas conexiones son permanentes.

Para obtener una conexión, una persona ha de firmar un contrato, y dar su nombre, dirección y otros datos personales. Por regla general, el usuario recibirá un nombre de identificación de usuario, que puede ser un seudónimo, y una contraseña, con lo que nadie más podrá utilizar su abono. Aunque sólo sea por motivos de seguridad, los proveedores de acceso a Internet parecen registrar siempre en un fichero, de forma sistemática, la fecha, la hora, la duración y la dirección IP dinámica que se ha dado a un usuario de Internet.

Las empresas que actúan como proveedores de acceso a Internet a menudo ofrecen también servicios como proveedores de servicios de contenido de Internet. Por este motivo, el término genérico *proveedor de servicios de Internet* se utiliza en ocasiones para designar tanto a los proveedores de acceso como a los proveedores de servicios de contenido. No obstante, desde un punto de vista conceptual, los papeles que desempeñan son diferentes. Concretamente, el proveedor de acceso a Internet encaminará, en su calidad de vía de entrada a la Red, todo el tráfico que genere el usuario, mientras que el proveedor de servicios de contenido Internet sólo tendrá conocimiento de lo que suceda en sus servidores.

El usuario puede ser una organización, una administración pública o una empresa que utiliza Internet no sólo para proporcionar o hallar información, sino también para recoger datos que le sirvan en su trabajo o sus actividades, como procedimientos administrativos, venta de mercancías o prestación de servicios, publicación de guías, anuncios por palabras, envío de cuestionarios, etc[108].

[108] Documento de Trabajo "Privacidad en Internet":- Enfoque comunitario integrado de la protección de datos en línea –Adoptado el 21 de noviembre de 2000, https://212.170.242.148/upload/Canal_Documentacion/legislacion/Union%20Europea/Articulo%2029/2000/Documento%20de%20trabajo.%20Privacidad%20en%20Internet.%20Enfoque%20comunitario%20integrado%20de%20la%20protecci%F3n%20de%20d.pdf, (última visita 2 de Junio 2005).

Con respecto a las obligaciones de registro que tienen los Prestadores de Servicio de Internet hay que tener en consideración que no existe un único cuerpo normativo que regule los deberes de registro que tienen los ISP. Es por ello que distinguimos las obligaciones que impone la autoridad administrativa, a través de sus resoluciones exentas, y los deberes de registro que son impuestos por la ley, específicamente con la reforma al Código Procesal Penal (ley 19.927) .

3.3 Modificación al Código Procesal Penal en materia de Registro de datos de los usuarios.

La modificación al Código Procesal Penal y Código de Procedimiento Penal tiene lugar producto de la situación coyuntural producida por los casos de pornografía infantil y pedofilía. Con dicha normativa se quiere dotar de mecanismos para que los delitos puedan ser perseguidos.

Ahora bien, toda investigación penal tiene en la mira la determinación de los hechos constitutivos del delito y principalmente la detección de los autores, para ello resulta imprescindible contar con medidas que permitan la identificación de los sujetos que participan de los hechos punibles, lo que deviene en una limitación a la garantía del usuario a la privacidad. Los parámetros de estas restricciones a un derecho fundamental de los usuarios se discuten en Chile en sede legal en la ley 19.927, la llamada Ley de Pedofilía, en donde se imponen mandatos de control y registro a cargo de los ISP. Dicha norma con la modificación señala lo siguiente: Art.222 inc. 5º: *"Las empresas telefónicas y de telecomunicaciones deberán otorgar a los funcionarios encargados de la diligencia las facilidades necesarias para llevarla a cabo, en el menor plazo posible.* ***Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro no inferior a seis meses, de los números IP***

de las conexiones que realicen sus abonados. *La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento".* (La modificación en negrita).

Este tema de los deberes de registro produce gran discusión y debate en otras latitudes. A modo de ejemplo, en España la ley de la sociedad de la información permite que sea un reglamento el que fije la categoría de datos que deben ser guardados, y los plazos en que deben ser conservados[109].

En el mes de Marzo de 2005 el Defensor del Pueblo de España pidió medidas para limitar el anonimato en la Red. La petición consistía en obligar a los proveedores españoles de servicios de Internet a retener durante al menos un año los datos de conexión y tráfico generados por las comunicaciones de sus usuarios, para facilitar así la investigación frente a delitos de pornografía infantil, debido a que Internet al facilitar el anonimato haría de la pornografía infantil un delito impune. En concreto, pidió que en el desarrollo reglamentario del artículo 12 de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI): "*1- Que los ISP tengan que guardar los datos de conexión y tráfico de los internautas para facilitar las investigaciones. 2- Que la entrega de esos datos a los Cuerpos de Seguridad del Estado se efectúe cuando éstos actúen en cumplimiento de las funciones de carácter preventivo , esto es, sin necesidad de autorización judicial previa. 3- Que los ISP tengan la obligación de comunicar a los Cuerpos de Seguridad la existencia de cualquier contenido de carácter delictivo que detecten en sus servidores. 4- Que todos aquellos establecimientos denominados 'cibercafés' o 'cibercentros' lleven un control de los usuarios que usan sus servicios,*

[109] Artículo 12 de la ley de la Sociedad de la información número 4-Reglamentariamente, se determinarán las categorías de datos que deberán conservarse según el tipo de servicio prestado, el plazo durante el que deberán retenerse en cada supuesto dentro del máximo previsto en este artículo, las condiciones en que deberán almacenarse, tratarse y custodiarse y la forma en que, en su caso, deberán entregarse a los órganos autorizados para su solicitud y destruirse, transcurrido el plazo de retención que proceda, salvo que fueran necesarios para estos u otros fines previstos en la Ley.

registrando al efecto la persona que utiliza el puesto de acceso a Internet, y la franja horaria que utilizó" [110].

La crítica no se hace esperar. La Asociación de Internautas de España señala que se está confundiendo la obligación de retener los datos (que no afecta al secreto de las comunicaciones) con que tales datos pasen a estar disponibles para terceros ajenos al servicio concreto que posibilita esa retención de datos. Como condición inexcusable, debe existir la autorización judicial que posibilite el levantamiento del secreto de forma fundada, puesto que fue el constituyente quien erigió a los jueces y magistrados en garantes del secreto de las comunicaciones, de las que no pueden quedar excluidas las comunicaciones electrónicas.

En lo referente a los cibercafés o cibercentros, lanzar la sospecha de que pueden servir de medio para cometer los delitos más viles, y que por ello deba monitorizarse toda su actividad, no tiene otro significado que ser preludio respecto de cada terminal telefónico, punto de acceso, servidor de Internet, servidor de correo electrónico, porque desde todos ellos también puede delinquirse y además vilmente. La lucha contra la delincuencia, que prostituye los valores más básicos y esenciales de una sociedad, no puede ser la avanzadilla para dejar fuera del ámbito del secreto de las comunicaciones a las que se producen por vía telemática[111].

---

[110] El Defensor del Pueblo alerta del incremento de páginas web con pornografía infantil, Las Provincias, Valencia, España, 18 Febrero 2005, http://www.defensordelpueblo.es/herramientas/admin_noticias/uploads/Las%20Provincias%2018-02-05.pdf, última visita 4 Agosto 2006. Del mismo modo se publicó: El Defensor del Pueblo pide medidas para limitar el anonimato en la Red, El navegante, Madrid, España, Miércoles, 16 de Marzo de 2005 http://www.elmundo.es/navegante/2005/03/16/esociedad/1110980132.html, (última visita 2 de Junio 2005).
También información en "Revista del defensor del pueblo en España", Febrero 2005, N 4, pág. 5 http://www.defensordelpueblo.es/revista_prensa/revista_feb_05.pdf , (última visita 2 de Junio 2005).

[111] Asociación de Internautas, "La retención de datos y el secreto de las comunicaciones", 17-03-2005 http://www.internautas.org/html/1/2790.html, (última visita 2 de Junio 2005).

Detrás de esta discusión está el síntoma de considerar a todos los usuarios de Internet como potenciales delincuentes, y es más a los cibercafés como lugares de potenciales delitos, es la idea del peligrosismo detrás de Internet.

Volviendo a Chile, el funcionamiento eficaz del sistema requiere límites de actuación claros para que no se vulnere la privacidad de los usuarios y, en los supuestos que estos se deban limitar en virtud de otros intereses, dichas limitaciones se presenten como necesarias y apropiadas[112] para los fines específicos que se establezcan. Se presenta como necesario señalar que no parece apropiado que los deberes de control y registro de los ISP se establezcan sólo en el Código Procesal Penal por cuanto contribuye a crear inseguridad jurídica. En la tramitación de la ley 19.927 no se presentan mayores discusiones respecto a la norma que obliga a los ISP a mantener registros de los números IP de las conexiones. Es más, en el proyecto original, no se contemplaba esta obligación. Sólo una vez que exponen ante el congreso los representantes de la brigada del Cibercrimen es que se plantea la obligación de mantener estos registros. Esta señaló que serían especialmente útiles establecer el agente encubierto y el registro nacional de rangos de IP del proveedor junto al tiempo de almacenamiento del registro de IP. Luego, a través de una indicación del Senador Viera-Gallo, se introduce el texto actual[113]. Mayor análisis respecto a la norma no existe en la historia de la ley. Los parlamentarios, desde el momento que se les señala la utilidad que presenta, el registro, se muestran conformes [114].

---

[112] En la Directiva 2002/58/ se señala en el artículo 15 que "*la limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas"*

[113] Es en el Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento en que se introduce la obligación de registro de los IP de los usuarios. Es más de acuerdo al reglamento del Congreso todos los artículos votados por unanimidad respecto de los cuales no se haya pedido discusión o votación separada se pueden dar por aprobados. Esto es propuesto por el presidente de la sala y es aceptado. El senador Viera-Gallo explica que se introduce el registro de los números IP, tras lo cual se aprueba. Diario de sesiones del Senado, legislación 350ª extraordinaria, sesión 4ª, miércoles 13 de Octubre del año 2003, p. 30.

[114] BOLETÍN N° 2906-07 que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal, en materias de delitos de pornografía infantil.

Consideramos que toda regulación al respecto no debe tomar al usuario de Internet como el ser peligroso[115], como potencial delincuente al cual hay que controlar toda vez que el hecho que el usuario de Internet se presente como un sujeto anónimo no es en sí mismo reprochable, y es más se presenta, ese anonimato, como un Derecho que debe ser tutelado por el ordenamiento jurídico.

Una regulación sobre las responsabilidades, y los deberes de registro de los ISP como la existente en Chile, segmentada solo a la ley 19.927, genera miedo en el sistema, en cuanto a que los proveedores no tienen claridad sobre sus deberes y los usuarios ven limitados sus derechos. El miedo se traduce en inseguridad jurídica. Se presenta como necesario un marco normativo que procure dar seguridad jurídica y confianza tanto para los proveedores de servicio como para los usuarios.

4. Análisis Comparado sobre el marco normativo de los Prestadores de Servicios.

Para tener alguna idea sobre las normativas que en la actualidad están vigentes realizaremos un análisis comparado sobre la regulación estatal sobre los Prestadores de Servicios de Internet. Veamos, en primer lugar, el caso de Alemania. La regulación estatal se rige por la *Tele Service Act* que principalmente señala[116]:

- Los proveedores serán responsables según las leyes generales por sus propios contenidos, que ellos hacen disponibles al uso.

---

[115] BRUERA, Matilde, Bruera, Hugo *"Derecho Penal y garantías individuales: Registros penales y autoritarismo*", Editorial Juris. Rosario, Argentina, p. 132.

[116] Koenig, Christian, Ernst Röder and Sascha Loetz , "*The Liability of Access Providers. A proposal for regulation based on the rules concerning access providers in Germany".* International Journal of Communication, Law and Policy. Issue 3, 1999. http://www.digital-law.net/IJCLP/3_1999/pdf/ijclp_webdoc_7_3_1999.pdf , (última visita 15 Mayo 2007), p. 6. (Traducción propia).

- Los proveedores no serán responsables por cualquier contenido de un tercero que ellos hagan disponible al uso, a menos que ellos tengan conocimiento de dicho contenido y sean técnicamente capaces, y razonablemente se espere, que bloqueen el uso del contenido.
- Las obligaciones, de acuerdo a leyes generales, para bloquear el uso del contenido ilegal se mantendrán indiferentes si el proveedor obtiene conocimiento de dicho contenido cumpliendo con el secreto de las telecomunicaciones bajo el Artículo 85 de la Acta de Telecomunicaciones y su bloqueo es técnicamente factible y razonablemente esperado.

En primer lugar, vemos como la responsabilidad de los Prestadores de Servicios de Internet se rige por las normativas generales. En este sentido, la normativa indica que las situaciones a las cuales se verán expuestos los Prestadores no difieren en lo sustancial de los deberes y obligaciones que se deben cumplir en el entorno físico y no sólo virtual. Luego se señala que ellos deben ser responsables por sus propios contenidos. Efectivamente, en esta hipótesis nos encontramos frente a un sujeto que tiene las categorías de responsable tanto del contenido como de su publicación en la red. Es decir, por ser contenidos que se generan en el mismo entorno del ISP, haciendo posible su disposición pública, la responsabilidad recae doblemente en ellos.

A continuación , se menciona que los Prestadores no serán responsables, en principio, de los contenidos provistos por terceros. Se entiende que en estos casos el Prestador sólo actúa como medio para que el contenido esté disponible en Internet. De este modo, se reconoce el estatus mediático de los ISP. Esto mismo es lo que lleva a reconocer las contra excepciones. Sí ellos conocen el contenido y este representa un atentado contra las normativas generales, ellos ya no sólo actúan de manera mediática, sino que recae en ellos una responsabilidad por el hecho de tener conocimiento que a través sus servicios se están promoviendo contenidos, que de una u otra manera son contrarios al ordenamiento jurídico.

Además, se señala que estén en las capacidades técnicas de bajar o bloquear dicho contenido, lo cual no es más que la expresión de la lógica que a nadie puede exigirse más de lo que puede realizar. Hay que agregar que existe un elemento de racionalidad, al considerar los contenidos que "razonablemente" se espera que se bloqueen. Consideramos que esto último da el margen de flexibilidad necesario para aplicar principios preventivos a la protección de contenidos de Internet. De este modo, no siempre será necesario el requerimiento de un particular o del estado para esperar a que el contenido se bloquee. Tiempo en el cual, el bloqueo del contenido ya puede resultar inoficioso dada la naturaleza vertiginosa de la red.

Por último, se hace una referencia a la posibilidad de conocimiento de contenidos ilegales mediante el secreto de las telecomunicaciones. Nuevamente se hace además referencia a la factibilidad técnica y al elemento racional de poder bajar los contenidos. En este sentido, se da una preferencia al bloqueo de dichos contenidos en el caso que los proveedores lo detecten por sobre los conceptos del secreto de su transmisión.

En el caso español, la responsabilidad de los Prestadores de Servicios de Internet la podemos ver reflejada en la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico. En efecto, dicho cuerpo legal contempla en su Título II capítulos 2 y 3, una profusa reglamentación sobre los derechos y deberes con los cuales deben cumplir los Prestadores de Servicios. Así se reglamentan materias tales como la libre prestación de servicios, las restricciones a la misma y otras obligaciones junto al régimen de responsabilidad de los Prestadores de Servicios.

Un aspecto interesante al respecto son las numerosas regulaciones a las cuales se ven afectos los Prestadores de Servicios tales como medidas de publicidad respecto de quien es el ISP (artículo 10), deber de colaboración (artículo 11) y retención de datos (artículo 12). Sin embargo, a efecto de nuestro análisis nos detendremos en el régimen

de responsabilidad de los Prestadores de Servicios de Internet. En particular en su artículo 14, que señala:

"Artículo 14. Responsabilidad de los operadores de redes y proveedores de acceso.
1. Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos.
No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos, que tiene lugar durante su transmisión.
2. Las actividades de transmisión y provisión de acceso a que se refiere el apartado anterior incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello"[117].

En primer lugar, vemos que en el apartado número 1 se hace referencia a la idea de mero intermediario de los contenidos electrónicos. De este modo, se vuelve a ver la idea que previamente habíamos analizado en la legislación alemana. En este sentido, se da la contra excepción a la exención de responsabilidad: si los Prestadores de Servicios han tenido alguna injerencia en los contenidos, ya sea mediante el origen de la transmisión, modificación o selección de datos o de los destinatarios, ellos serán responsables por sus contenidos. Se trata, como ya habíamos mencionado, de un caso en donde los Prestadores pasan de ser meros comunicadores a actores de los contenidos pudiendo influir en su transmisión directamente.

[117] Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 14.

El segundo apartado recoge la misma idea del inciso final del número 1, al referirse a los procedimientos técnicos que se requieren para la transmisión de datos. Es de entender que para el manejo y transmisión de datos los Prestadores de Servicios deben necesariamente pasar por el manejo automatizado del contenido. Pero, por lo mismo, este manejo es ajeno a cualquier intervención humana, y por ello se excluye del término de intervención o participación de las comunicaciones que da origen a su responsabilidad. De hecho en el artículo siguiente (15) también se hace mención a la exención de responsabilidad de los Prestadores en el caso que por diversos motivos señalados en la ley, éstos tengan que almacenar datos de sus usuarios y este almacenamiento se realice de manera automatizada.

Luego, en el artículo 16, la legislación española hace referencia a la idea del conocimiento efectivo del contenido de los datos y de disponer de los medios técnicos para su eliminación. Se hace referencia a la actuación con diligencia de los Prestadores de Servicios en eliminar o bloquear los contenidos, cambiando la idea del elemento racional por el de diligencia. Sin embargo, nuevamente las ideas de las directivas europeas se mantienen en su esencia, y tal como lo vimos en el caso alemán, son principios de base y aplicabilidad general que pueden permitir el mayor compromiso con libertad de los Prestadores de Servicios de Internet.

Cabe hacer una pequeña mención al apartado 1 inciso final, que, a propósito de la responsabilidad por el alojamiento de datos, señala: *"Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución,* ***sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que***

pudieran establecerse"[118]. Interesante mención a las posibilidades de autorregulación que analizamos anteriormente.

Para finalizar con nuestro análisis comparado, veamos algo de lo que nos indica la legislación norteamericana al respecto. Para ello nos basaremos en la Digital Millenium Copyright Act, de 1998, que implementa dos tratados de la Organización Mundial de Propiedad Intelectual de 1996 y variados tópicos relacionados.

La referencia a la que haremos mención se encuentra en el título II, sección 512, sobre la limitación de responsabilidad relativa al material en línea. Al respecto, cabe señalar que la legislación norteamericana sigue reglas similares a las analizadas anteriormente. De este modo, señala que los Prestadores de Internet no serán responsables por infracciones al derecho de autor siempre y cuando la transmisión hubiese sido originada en un tercero, de manera automatizada, cuando el Prestador no selecciona al receptor y otras situaciones que en general se refieren a la no intervención del Prestador en el contenido sino como mero ente transmisor[119].

---

[118] *Ibid.* Artículo 16 n° 1.

[119] La mencionada sección señala: "*TRANSITORY DIGITAL NETWORK COMMUNICATIONS- A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if--*
(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
(5) the material is transmitted through the system or network without modification of its content." Digital Millennium Copyright Act. Título II, Sección 512.

Algo similar se contempla en relación al *caching,* información residente en sistemas o redes de direcciones de usuarios y sistemas de búsquedas, las cuales no reproducimos por el extenso contenido de las regulaciones. Sin embargo, atienden al elemento de participación, conocimiento y factibilidad técnica de bloqueo de los contenidos. Confirmando con esto la tendencia a reafirmar los principios sobre la injerencia de los Prestadores en los contenidos y las comunicaciones.

Como conclusión de la presente sección, podemos señalar que la responsabilidad de los Prestadores de Servicios de Internet en el derecho comparado parece seguir las mismas líneas de responsabilidad, que van de acorde a las necesidades operacionales de la red. Esto es, no dificultando la rapidez y eficiencia de los contenidos de la red, defendiendo al mismo tiempo los derechos de las personas, en la medida que los Prestadores tengan conocimiento de las infracciones. De otro modo, podríamos caer en la situación que los Prestadores de Servicios de Internet se convirtieran en verdaderos policías de la red, ya que al hacerlos responsables por todo el contenido que ellos transmitan, de una u otra forma se protegerían revisando las comunicaciones y con ello vulnerando el derecho a la privacidad de sus comunicaciones.

Capítulo III. Hipótesis de Riesgo.

Como mencionamos al iniciar este trabajo, para conocer y poder delimitar los alcances de la protección al derecho al anonimato, debemos saber hasta qué punto se pueden sacrificar los derechos del usuario en diversas hipótesis de riesgo. En otras palabras debemos analizar cómo y bajo que circunstancias es posible intervenir las comunicaciones de las personas y guardar registros de las mismas. Para esto analizaremos diversas situaciones en las cuales el derecho al anonimato se puede ver comprometido.

Partimos con una conceptualización acerca del contenido nocivo y el contenido ilícito, para seguir con un estudio a la Ley de Pedofilía en cuanto a las obligaciones de guardar registro por los proveedores de acceso a Internet. Continuamos con un examen a los contenidos referentes a los registros de datos de tráfico y facturación. Posteriormente nuestra hipótesis de riesgo abordará la situación de posibles conflictos en el marco de la Ley de Propiedad Intelectual, teniendo en cuenta su modificación para adecuarla al TLC. Finalmente nos enfocaremos al tratamiento de los datos, concluyendo con dos hipótesis de riesgos referidas a las cláusulas contractuales y las políticas de requerimiento.

1. Definición de Contenido Ilícito y diferencia con el contenido Nocivo.

El contenido ilícito es aquel que es constitutivo de delito. Para calificar si una determinada información en la red es un contenido ilícito, hay que revisar la legislación penal de cada Estado. En cambio, los contenidos nocivos son aquellos que no violan la norma penal pero pueden atentar contra la moral o las buenas costumbres de la sociedad, en un momento dado. El material o información nociva expresa opiniones o creencias políticas, religiosas y culturales que pueden ser consideradas ofensivas respecto de

terceros.[120] El contenido nocivo va a depender de lo que una determinada comunidad estime como indebido. Así, una comunidad o sociedad conservadora considera nocivo un determinado tipo de información, mientras otra comunidad, de tono más liberal, no encontrará nocivo el mismo tipo de información.

La determinación de lo que se considera un contenido ilícito es más sencilla ya que *"los contenidos ilícitos permiten una delimitación más ajustada, por la sanción penal que envuelven dichas conductas en cada país, en las que existe cierto «consenso internacional"*[121]. Con estas definiciones queda expresado que contenidos ilícitos y nocivos no son sinónimos[122].

Teniendo esto como base, las hipótesis de riesgo a analizar las configuraremos en torno a lo que son las infracciones a los Derechos al Honor y a la propia imagen.

---

[120] Dictamen del Comité de las Regiones de 13 de marzo de 1997 sobre el "Libro Verde sobre la protección de los menores y la dignidad humana en los nuevos servicios audiovisuales y de información" (doc.COM (96) 483 final) y la "*Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones-Contenidos ilícitos y nocivos en Internet* (doc. COM (96) 487 final) http://www.cor.eu.int/coratwork/comm7/spanish/440-96.htm; (última visita 20 junio 2005)

[121] PRADO, Arturo, *"Los Contenidos Ilícitos y Nocivos de Internet",* revista del Colegio de Abogados, N° 26, Noviembre del 2002. Entre los cuales cabe mencionar *la apología al terrorismo, la pornografía infantil, la provocación o incitación al odio de una raza, etnia o grupo, la difamación on line claramente maliciosa y la distribución de material soez que viola la dignidad humana.*
http://www.colegioabogados.cl/revista/26/articulo11.html , (última visita 8 de Diciembre 2004)

[122] MORALES, Fermín, "Pornografía infantil e Internet", Ponencia de las Jornadas de Responsabilidad Civil y Penal de los Prestadores de Servicios en Internet (Barcelona, 22-23 de noviembre de 2001), http://www.uoc.edu/in3/dt/20056/index.html, última visita 3 de Junio 2005. *"Se alude a contenidos ilícitos y nocivos en Internet como si de un mismo problema se tratase, cuando en realidad se trata de dos categorías conceptuales de contenidos diversos. Las medidas jurídicas de respuesta a la difusión de contenidos ilícitos, entre ellos el tráfico de pornografía infantil, reclaman respuestas jurídicas puntuales enderezadas a sancionar la fuente originaria de tal difusión. Por el contrario, los contenidos nocivos constituyen un concepto más difuso, que alude a la necesidad de generar pautas culturales en la Red tendentes a sensibilizar a los usuarios, para lograr así la paulatina erradicación de aquéllos."*

-Nuevas formas de afectación al honor en la Red.

Procederemos a analizar tanto una serie de conductas que se dan en el mundo virtual por parte de los usuarios de la Red, como el surgimiento de nuevos "servicios" y lo que se ha denominado también como comunidades virtuales.

Lo que será analizado son los foros en Internet, los blogs, y los fotolog. Debemos tener presente que estas hipótesis dentro de lo que hemos agrupado como contenido ilícito, no son todas las conductas que pueden suscitarse en la Red.

No es el objetivo revisar con detalle la normativa que regula la Responsabilidad de los ISP. El objetivo es determinar las expectativas de privacidad que tienen los usuarios. Para ello se nos presenta como necesario explicar bajo que condiciones y supuestos se presentan y creemos se presentarán los mayores problemas. Sin embargo ello nos lleva a tocar la responsabilidad de los ISP.

El debate en torno a infracciones al Derecho al Honor y a la propia imagen, se desarrolla en torno a reclamaciones contra proveedores de servicios de Internet por mensajes con contenido difamatorio o injurioso, o también la publicación de fotografías íntimas. Esto, generalmente ocurre en los llamados foros de discusión. Sobre el funcionamiento de estos foros hay que realizar algunas precisiones. Existen foros en los cuales existe un moderador y otros en los cuales no está presente un moderador. Un error frecuente al respecto es considerar que la existencia de un moderador equivale a la de un editor y de esa manera hacer responsable al prestador de Servicios de Internet.

La distinción entre foros con moderador y sin moderador no nos sirve para determinar la responsabilidad del prestador de Servicios de Internet. Esto porque se caería en una contradicción que sigue la siguiente lógica: El foro que no tiene moderador

no es responsable por los contenidos ilícitos o nocivos que difundan los usuarios de los foros. Luego, estos prestadores de servicios a lo más tienen el deber general de colaborar con la justicia para identificar a los autores del contenido con carácter de difamatorio. En cambio, el foro al tener un moderador se podría entender que al contener un contenido de carácter ilícito es porque el moderador lo permitió. Luego el moderador incurrió en una omisión de sus deberes de cuidado y por ello se hace responsable el prestador de Servicios de Internet. Este argumento es ilógico por cuanto implicaría que a los prestadores de Servicio no les convendría poner moderadores a estos foros, siendo que la presencia de estos garantiza de mejor manera la protección jurídica de los bienes jurídicos aquí señalados, además de dar orden a estos foros.

La función de los moderadores no tiene relación, muchas veces, con determinar si el contenido de los mensajes puede acarrear responsabilidad civil, sino sólo a catalogar que el mensaje se corresponda con la materia que trata el foro. Para reafirmar esto se ha expresado que "*los efectos de atribuir responsabilidad al proveedor en la medida en que su foro es moderado, no impide apreciar que si bien la función del moderador es controlar qué mensajes son difundidos, su selección – en un contexto, caracterizado por la multiplicidad de mensajes, la participación de diversos servidores en la difusión de los foros, la heterogeneidad de los participantes en la Red y la velocidad a la que se sucede la publicación de mensajes- se ciñe en muchas ocasiones a comprobar que el mensaje se corresponde con la materia a la que se refiere ese foro, sin analizar su contenido y, en particular, que éste puede generar responsabilidad civil"*[123].

Todo esto, unido a que Internet crece de forma exponencial, lleva a que controlar toda la información que se genera a diario sea económicamente inviable.

[123] MIGUEL ASENCIO, Pedro Alberto, *"Derecho privado de Internet",* Editorial Civitas, Madrid, 2001. p. 532.

Así, aún cuando en un foro determinado exista un moderador el prestador de servicios de Internet no tiene deberes de vigilancia sobre los contenidos que circulen en su foro. La ley no le establece deberes de vigilancia al respecto. "*No se ha señalado norma alguna que establezca esta obligación de cuidado respecto de los proveedores de acceso para exigirles que adopten una conducta de vigilancia permanente respecto del contenido de la red"*[124].

El otro fenómeno que debe ser analizado es lo que acontece con los weblogs o blogs. El Blog es, en términos sencillos, una especia de diario de vida pero de carácter público creado por un sujeto para hablar de distintos tópicos[125].

A estos se le asocia a cierto ideal romántico liberal, ya que permite el debate público, que se ha perdido en la democracia actual[126]. Pero también puede generar problemas en el ámbito de los contenidos. Hay blogs que sólo hablan de la vida privada del sujeto haciendo de ella algo público, mientras otros se discute temas de política, ciencia o arte.

El que sea un espacio, o mejor llamado un ciberespacio en que se permite la discusión es lo que hace señalar que es una forma de discurso público que afianza a la sociedad civil. Esto hay que entenderlo en su estrecha relación con la libertad de expresión por cuanto "*buena parte de las leyes acerca de la libertad de expresión tienen como finalidad el preservar espacios en los que pueda darse la disensión. (...) La Ley constitucional protege, en el espacio real, el derecho de los apasionados y de los*

---

[124] MATURANA, Cristian "Responsabilidad de los proveedores de acceso y de contenidos de Internet", Revista Chilena de Derecho Informático N° 1, Santiago, Chile, p. 25.

[125] Una definición que suele ser mencionada y que sirve de referente en el estudio de los blogs es la que entrega la Wikipedia que señala que "*Un weblog, también llamado blog o bitácora, es un sitio web donde se recopilan cronológicamente mensajes de uno o varios autores, sobre una temática en particular o a modo de diario personal, siempre conservando el autor la libertad de dejar publicado lo que crea pertinente"* http://es.wikipedia.org/wiki/Weblog., (última visita 15 Agosto 2005).

[126] El análisis que se realiza es respecto a debates políticos, como una nueva forma de periodismo que no tendría el conflicto de intereses de los medios tradicionales de información. Sin embargo también se da en todos los ámbitos de la cultura.

"bichos raros" a dirigirse a todos los demás miembros de la sociedad. En el espacio real existen lugares donde la gente se puede reunir y en los cuales es posible repartir folletos propagandísticos. (……). Nuestras sociedades se han convertido en sociedades tan apolíticas que si decidiésemos ejercer en la realidad este derecho protegido por la constitución, todo el mundo pensaría que nos hemos vuelto locos de atar"[127].

Lo que sucede en estos ciberespacios denominados blogs es que los usuarios pueden debatir de una diversidad de temas con la vehemencia que quieran, pueden defender sus ideas sin ser considerados locos por ocupar sus derechos a expresarse en un lugar público, además de interactuar en el tiempo mediante la comunicación electrónica[128].

¿Cómo se evita en Internet cualquier vulneración del honor de las personas cuando éste es agredido a través de informaciones que tienen el efecto de multiplicarse?. Las páginas retienen informaciones durante mucho más tiempo que los medios tradicionales como los periódicos o la televisión.

En EE UU, que es un parámetro a analizar para la búsqueda de soluciones a este tipo de problemas, se tiene claro que la forma de resolverlos es aplicar con carácter general la jurisprudencia, ya establecida para los demás medios de comunicación tradicionales[129].

---

[127] LESSIG, Lawrence, *"El código y otras leyes...",* Op. cit. p. 135-136.

[128] LESSIG lo plantea en términos que la gente publica cuando quiere publicar y lee cuando quiere. Las tecnologías que hacen posible una comunicación no sincrónica, tales como el correo electrónico, incrementan las oportunidades para la comunicación. LESSIG, Lawrance, "Cultura libre...", Op.Cit. p.56.

[129] MUÑOZ MACHADO, Santiago, en "La libertad y el poder en Internet", plantea que lo que se dijo en el "New York Times versus Sullivan es lo que se está aplicando en Internet. Y aún así, parecería que no basta; de hecho, en algunos países europeos se están añadiendo supuestos específicos y relativos sólo a Internet a esa jurisprudencia, a esos sistemas de respuesta tradicionales. En Alemania, se ha llevado a cabo este procedimiento a partir de la regulación de una ley de 1997 que establece algunas modificaciones de esas respuestas tradicionales para exigir, por ejemplo, que cuando un afectado por una noticia en Internet pretenda rectificarla, no sólo tenga el derecho a rectificación, sino también a que ésta permanezca expuesta en el mismo sitio donde ha surgido la difamación y al menos tanto tiempo como la difamación se produjo. Todo esto que parece tan complicado no es nada más que una adaptación de lo habido a un

En lo que respecta a la relación que existe entre los blog y el periodismo tradicional hay que señalar que los primeros no tienen un carácter profesional[130] y si bien en un principio fueron mal mirados, en el último tiempo se los señala como un nuevo poder.

Para ejemplificar lo anterior señalamos un hecho noticioso del año 2005. En Febrero del año 2005 se tituló en diferentes portales de Internet lo siguiente: "EL PODER DE LOS WEBLOGS COBRÓ SUS PRIMERAS VÍCTIMAS"[131]. Este titular trata la noticia del hecho que tres periodistas habían tenido que dejar su trabajo debido a situaciones que afectaban su credibilidad y ética como periodistas.

Un caso fue el de un reportero de un medio periodístico estadounidense llamado Talon News Service. Este sujeto realizaba su labor en la Casa Blanca y comenzó a levantar sospechas entre sus colegas, al ser identificado como el periodista predilecto del presidente, ya que realizaba sus preguntas en los momentos más difíciles para el entrevistado. El momento que marcó el punto de inflexión fue cuando George W. Bush lo seleccionó para realizar una pregunta, la que formulo estando totalmente fuera de contexto, con lo que ayudó a cambiar de rumbo la conversación.

Americablog.org, fue el blog que reveló que Guckert (nombre del pseudoperiodista de Talon News Service) se dedicaba a la prostitución masculina cobrando 200 dólares a la hora. Tenía su propio sitio web donde promocionaba sus 'servicios'. Antes de ingresar a la Casa Blanca como periodista acreditado, tomó un curso de dos días para poder 'adquirir' las habilidades que exige el periodismo y la empresa para la cual trabajaba era propiedad de un miembro del partido republicano.

---

instrumento de comunicación nuevo que es Internet. Transcripción de el aula de la cultura virtual en http://canales.elcorreodigital.com/auladecultura/santiago5.html, (última visita 2 de Junio de 2005).

[130] LESSIG, Lawrence, "Cultura libre", Op. cit. p. 58. Señala que son amateur no en el sentido de falta de experiencia sino en el sentido de que son sujetos a quien no se les paga para que informen.

[131]El poder de los weblogs cobró sus primeras víctimas, 22 de Febrero 2005, http://www.terra.cl/tecnologia/index.cfm?id_reg=466997&id_cat=415&accion=internet, última visita 5 marzo 2005.

Lo que se quiere resaltar de este caso es que no fueron los colegas de la propia prensa por los medios tradicionales los cuales difundieron la noticia de este pseudoperiodista, sino que fue en los blogers donde se realizó. El porqué no fue la prensa la que reveló este hecho se explica ante el miedo de perder las acreditaciones para reportear en la Casa Blanca.

No se niega el hecho de que en los blogers trabajen periodistas, sino que la situación de libertad y el no tener conflictos de intereses les permiten afrontar estas situaciones descritas y revelar lo que podrían ser prácticas poco éticas.

Esa es una cara de los blog. La otra cara es que los blogers tienen un interés central, el cual es que los visiten. Para ello, muchas veces utilizan material protegido por las leyes de propiedad intelectual o industrial sin autorización. También el hecho de que algunos de los comentarios que puedan aparecer sean ofensivos o injuriosos. El hecho de que aparezcan blogs defendiendo al nazismo, o negando el holocausto judío, haciendo apología del terrorismo, siempre genera controversia y una presión para que estos sean bajados.

Un derivado de los web logs son los fotolog, que consiste básicamente en una galería de imágenes fotográficas publicadas regularmente por uno o más autores. Generalmente, junto a cada foto, el dueño del fotolog pone comentarios referidos a ella. Normalmente aceptan comentarios en la forma de libro de visitas[132]. No hay estadísticas etáreas sobre los que utilizan esta plataforma. El único fotolog que contiene estadísticas etárea, hasta el momento, es un sitio belga llamado photoblog, del cual el grupo adolescente de 12 a 18 años ocupa cerca del 50% del total de los blogs[133].

---

[132] Hay datos interesantes en cuanto a la magnitud del fenómeno en "Fotolog." *Wikipedia, La enciclopedia libre*, http://es.wikipedia.org/w/index.php?title=Fotolog&oldid=4168754, (última visita 15 Marzo 2005).

[133] http://photoblog.be/?action=browse&id=age , al 15 febrero del 2005 de un total de 78.000 fotolog 43.000 pertenecían al grupo etáreo entre 12 y 18 años. Junto a destacar este hecho debemos indicar que en este fotolog belga el país con más miembros es Chile con cerca de 25.000 fotologs a la fecha.

La importancia de tratar este tema está dada porque en Chile los fotolog han tenido gran desarrollo. Lo cual queda manifestado en los dominios nacionales que se han creado, dentro de los cuales se tienen fotolog.cl[134] , jotelog.cl[135], y los servicios de fotolog que ofrecen algunos portales. Si uno considera que los blogs tienen una cara ligada a afianzar un discurso público, uno podría sostener que los fotolog constituyen una nueva plataforma de aprendizaje. Es una parte de lo se denomina alfabetismo mediático, que es la capacidad para entender, analizar y deconstruir las imágenes de los medios. La alfabetización ya no consiste sólo en leer y escribir, *"en un mundo en el que los niños ven, de media, 390 horas de anuncios en la televisión al año, entre 20000 y 45000 anuncios en general, es cada vez más importante entender la "gramática" de los medios. Porque igual que hay una gramática para la palabra escrita, hay también una para los medios[136].*

Lo anterior es una parte de lo que generan los fotologs. Para entender los problemas, que se suscitan con los fotolog, nos permitimos reproducir la lista de noticias referidas a un fotolog ocurrida en el mes de febrero de 2005.

El 23 de febrero del año 2005 se publica:*"Sitio web muestra a supuestas colegialas chilenas en eróticas poses. Sensual foto de alumna indigna al Liceo 1. La*

[134] http://www.fotolog.cl/ con 83.000 usuarios inscritos y 324988 fotos, última visita 15 de Febrero 2005.
[135] http://www.jotelog.cl/ , que a la fecha del 3 de marzo del 2005 contaba con 111.752 usuarios y 758.170 fotos.
[136]LESSIG, Lawrence, "Cultura libre", Op. cit p. 49. La importancia de lo que se ha dado en llamar alfabetización digital es entendido en Chile en términos aún débiles como un factor importante para reducir la brecha digital. Es así que el Ministerio de Educación tiene una campaña nacional de alfabetización digital, que se desarrollará en el período 2003-2005, y que tiene como objetivo capacitar a medio millón de chilenos mayores de 15 años que están fuera del sistema escolar para que obtengan formación práctica en el uso de las Tecnologías de Información y Comunicación (TIC).Se trata de preparar a la ciudadanía para vivir en una sociedad globalizada y aprovechar las oportunidades que ofrecen las nuevas tecnologías digitales. La iniciativa está dirigida a vastos sectores de la población que hasta hoy no han tenido acceso a la computación e Internet, especialmente trabajadores, microempresarios y madres.

imagen pertenecería a una estudiante de tercero medio. ...Me parece grave y en ningún caso ella nos representa", opinó Julia Alvarado, directora del colegio"[137].

El 24 de febrero del año 2005: *"La menor, de iniciales J.R., sospecha de un sujeto que le manda mensajes a su celular Alumna del Liceo 1: "Ver mi foto en internet me ha hecho mucho daño"*[138] *El 25 de Febrero la noticia es la siguiente: "Sitio Fotolog.cl optó por bloquear el link" Foto de liceana fue sacada de Internet*[139]*. Edson Lara, administrador del sitio afirmó que bloqueamos los links donde aparecía la niña. Allí salía sólo una foto de la escolar y las otras eran de una vedette vestida de escolar además señaló que entregarán los antecedentes que necesite la familia sobre el lugar desde donde fueron cargadas las fotografías. La decisión de eliminar las imágenes se deben a que esta es una propaganda negativa, primero que todo para las personas afectadas, en este caso el Liceo 1. Y también es negativo para el sitio presentar imágenes de este tipo".*

De esta manera se plantea la pregunta si el usuario tiene una expectativa razonable de privacidad ante el proveedor de servicios de alojamiento. Tomando con seriedad los hechos uno no puede dejar de hacer notar una cierta paranoia de diario sensacionalista.

Este tipo de caso, en que se ven involucradas fotografías, que pueden ser consideradas de carácter erótico o sensual debe ser diferenciado de las que correspondan

---

[137] Foncea, Sebastián, Sensual foto de alumna indigna al Liceo 1, Las Últimas Noticias, Chile 23 de Febrero 2005, http://www.lun.com/ElDia/detalle_noticia.asp?idnoticia=C384059095224653&cuerpo=701&seccion=801&subseccion=901 , (última visita 29 de Mayo del año 2006).

[138] Foncea, Sebastián, "ver mi foto me hace daño", Las Últimas Noticias, Chile, 24 de Febrero 2005. http://www.lun.com/ElDia/detalle_noticia.asp?idnoticia=C384068730135069&cuerpo=701&seccion=801&subseccion=901, (última visita 29 de Mayo del año 2006).

[139] Foncea, Sebastián, Foto de liceana fue sacada de Internet, Las Últimas Noticias, Chile, 25 Febrero 2005, Cihttp://www.lun.com/ElDia/detalle_noticia.asp?idnoticia=C384079118698958&cuerpo=701&seccion=801&subseccion=901, (última visita 29 de Mayo del año 2006).

a las de pornografía infantil, siendo ésta todo material audiovisual que utiliza niños en un contexto sexual. Uno no podría entender que producto de esta situación se dedicara el administrador a buscar y bloquear todos los sitios en que aparezcan menores con uniforme. Si entendemos que puede constituir una buena plataforma de aprendizaje no puede cercenarse con censura en todo momento. Además, sería prácticamente imposible detectar todas las fotos que provocan problemas al honor.

El administrador (en el caso planteado con anterioridad) tomó una alternativa para preservar el sitio y sacarse de encima los reclamos principalmente del diario. En cuanto a las expectativas de privacidad que tiene el usuario hay que tener presente que este debe inscribirse para poder utilizar el servicio. Datos sobre esa inscripción son dados en las mismas páginas. No es requisito que los usuarios inscriban datos verdaderos para participar del servicio.

La declaración en torno a entregar los antecedentes para determinar el lugar donde fueron cargadas las fotografías no hace más que establecer una regla de conducta a los usuarios que no se había dado hasta la fecha, como una norma de autorregulación, en cuanto a que los motivos que obligan a bloquear un sitio son comunicados al usuario y al resto de la comunidad del servicio, y luego a quién solicite los datos por una causa razonable serán facilitados, luego las expectativas de privacidad se mantienen en un estándar de razonabilidad establecido.

2. Revisión a la ley de pedofilía (19.927) y su implicancia en el entorno digital.

Toda investigación penal tiene en la mira la determinación de los hechos constitutivos del delito y la detección de los autores, para ello resulta imprescindible contar con medidas que permitan la identificación de los sujetos que participan en los hechos punibles.

En Internet su suscitan problemas debido al anonimato en que actúan los usuarios. Las medidas que se adoptan en miras de la persecución penal devienen en una limitación al derecho del usuario a la privacidad. Los parámetros de estas restricciones a un derecho fundamental de los usuarios se discuten en Chile en sede legal en la ley 19.927, la llamada Ley de Pedofilía, en donde se imponen mandatos de control y registro a cargo de los ISP.

2.1 Delimitación conceptual de la pornografía infantil.

La definición de lo que es pornografía infantil es compleja por cuanto depende de una serie de factores, dentro de los que se cuentan, ideas religiosas, creencias de orden moral, y pautas de comportamiento sexual. En el siguiente análisis partiremos de una serie de definiciones que se han dado en la legislación extranjera como nacional.

Una primera aproximación al concepto de Pornografía Infantil la encontramos en el protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (ratificada por Chile el 6 de Febrero de 2003) en su Artículo 2 c) señala que: *"Por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales"*[140].

[140] Protocolo facultativo de la Convención sobre los Derechos del Niño relativos a la venta, de niños, prostitución infantil y la utilización de niños en la pornografía del 18 de Enero del año 2002. Ratificado por Chile el 6 de Febrero de 2003, documento en línea en: http://www.cejamericas.org/doc/legislacion/tratados/onu-protocolo-facultativo-ninos.pdf, (última visita 31 Mayo del 2006).

En el contexto Europeo, el consejo de Europa define la pornografía infantil como: *"cualquier material audiovisual que utiliza niños en un contexto sexual"* [141].

En tanto, en el Convenio sobre la Ciberdelincuencia del Consejo de Europea define la Pornografía Infantil en el Artículo 9 N° 2 señalando que: *"Por pornografía infantil se entenderá todo material pornográfico que contenga la representación visual de: a) un menor comportándose de una forma sexualmente explícita; b) una persona que parezca un menor comportándose de una forma sexualmente explícita; c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita. 3 A los efectos del anterior apartado 2, por menor de edad se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años."*

Nuestra ley 19.846 sobre calificación cinematográfica en su artículo 2 d) define lo que se entenderá por contenido pornográfico como: *"La exposición abusiva o grosera de la sexualidad o la exposición de imágenes obscenas, con interacciones sexuales más o menos continuas que, manifestadas en un plano estrictamente genital, constituyen su principal fin".*

El artículo 366 quinquies del Código Penal señala: *"El que participare en la producción de material pornográfico, cualquiera sea su soporte, en cuya elaboración hubieren sido utilizados menores de dieciocho años, será sancionado con presidio menor en su grado máximo. Para los efectos de este artículo y del artículo 374 bis, se entenderá por material pornográfico en cuya elaboración hubieren sido utilizados menores de dieciocho años, toda representación de éstos dedicados a actividades sexuales explícitas, reales o simuladas, o toda representación de sus partes genitales con fines primordialmente sexuales".*

[141] Esta definición la entrega el Consejo de Europa, Recomendación nº R(91)11, de 9 de septiembre de 1991, del Consejo de Europa sobre la explotación sexual, la pornografía, la prostitución y el tráfico de niños y de jóvenes adultos. Con posterioridad se entrega la misma definición en el Convenio sobre la Ciberdelincuencia artículo 9 N° 2.

De todas las definiciones dadas, esta última intenta integrar a las demás. Debemos analizar esta norma para determinar cuál es el bien jurídico protegido en la legislación nacional.

Para interpretar la norma se debe determinar cuál es la finalidad de esta. La norma al emplear la expresión "toda representación", puede generar dudas en cuanto a si se incrimina lo que se conoce como pornografía técnica y la pseudopornografía infantil.

Pornografía técnica es aquella "protagonizada por mayores de edad que aparentan ser menores por muy diversos medios o procedimientos ("retoque" de fotografías o filmaciones consistentes en eliminación de vello pubiano o facial, suavización de facciones, empleo de vestimentas de adolescentes, etc.)"[142] .

Lo que procura la norma es amparar la indemnidad de los menores. Es por esto que no se incrimina la "pornografía técnica" por cuanto el tipo señala la idea de "utilización de los menores", no se sanciona "*la estricta actividad de creación de un material calificable objetivamente como de "pornografía relativa o alusiva a menores*"[143].

De la misma manera, quedan fuera de la normas las representaciones virtuales. En consecuencia, los dibujos o el empleo de otras técnicas, que aún cuando se refieran a menores, no pueden quedar comprendidos en la norma, dado que no están afectando la indemnidad de algún menor.

[142] MORALES, Fermín, "Pornografía infantil e Internet" http://www.uoc.edu/in3/dt/20056/index.html, (última visita 30 de Mayo del 2006).
[143] Ibíd.

En definitiva, debe tratarse de actos que afligen a "personas de carne y hueso".[144] Una interpretación distinta de la norma habría implicado vulnerar el principio de legalidad, toda vez que no se afecta ningún bien jurídico, y se habría transformado en una invasión a la intimidad de las personas [145].

Se entiende por pseudopornografía aquélla en la que se insertan fotogramas o imágenes de menores reales en escenas pornográficas (animadas o no), en las que no intervienen realmente.

En estos casos pueden presentarse problemas interpretativos, ya que se emplean menores a través de montajes. En muchos casos es difícil dilucidar si el material utiliza al menor en forma virtual o real.

Una postura es determinar cuál fue el comportamiento efectivo del menor, dado que si sólo se utilizó el rostro o su cuerpo y luego quien realiza el montaje lo representa —o, mejor dicho lo manipula— en actividades pornográficas, no se comprendería dentro de la norma. En consecuencia, sólo podría estimarse material pornográfico si el menor realiza las actividades sexuales descritas, las que luego se emplean en los dibujos u otras imágenes[146].

Una segunda postura, es que la pseudopornografía se comprende en el tipo. El razonamiento sigue la siguiente lógica. El bien jurídico tutelado no es el de la indemnidad del menor ni su libertad sexual sino su dignidad o su derecho a la propia

---

[144] Departamento de Estudios de la Defensoría Nacional penal. Comentarios la Ley 19.927 de Delitos de Pornografía Infantil, http://www.defensoriapenal.cl/index.php?seccion=6&id=37, (última visita 15 Junio 2005).

[145] MORALES Fermín. Ob. cit. p.4 "*La producción de pornografía infantil generada por ordenador (pornografía virtual) ha suscitado ya un hondo debate jurídico. Desde amplios sectores jurídicos se ha demandado que este tipo de pornografía no sea objeto de medidas incriminadoras, por cuanto en tales supuestos no se verifica una utilización real de menores, de modo que la prohibición del referido material supondría una injustificada y desproporcionada limitación a la libertad de expresión."*

[146] Departamento de Estudios de la Defensoría Nacional. Op. cit p.2.

imagen conectado con la idea anglosajona de privacidad. La norma de este modo protegería al menor a través de un derecho a su propia imagen [147].

Para entender cual es el bien jurídico tutelado tomamos la opinión de la jueza Verónica Sabaj, opinión en el proceso de formulación de la ley y recogida en el INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO[148]. De esta manera, señala que, en lo referente a los bienes jurídicos protegidos, existen tres conceptos específicos:

a) La libertad sexual, en el caso de personas mayores de 18 años, es decir, el derecho a no ser involucrado en una interacción sexual sin su consentimiento. Así, la libertad sexual, tal como está protegida en nuestro derecho, es una libertad de abstención sexual. La regulación penal utiliza distintos parámetros para proteger la libertad, correlacionando fundamentalmente dos variables: la edad de la víctima y los medios de ataque.

Tratándose de personas mayores de 18 años, el sistema penal dispensa protección penal frente a casos graves de afectación de su libertad, principalmente a través del uso de medios coercitivos denominados "fuerza o intimidación".

b) Indemnidad sexual en el caso de las personas menores de edad púberes, esto es la protección del Estado que se traduce en castigar la manipulación de la voluntad del menor mediante engaño u otras formas graves de abuso, tratando así de evitar experiencias perturbadoras.

c) Intangibilidad sexual para el caso de las personas menores de edad impúberes, en virtud de la cual la interacción sexual con un menor impúber es punible,

[147] MORALES, Fermín. Ob. cit. p.4. Esta interpretación es minoritaria.
[148] INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO recaído en el proyecto de ley, en segundo trámite constitucional, que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal, en materias de delitos de pornografía infantil. BOLETÍN N° 2906-07

independientemente de los medios comisivos o de la concurrencia de ciertas circunstancias de comisión.

De estas consideraciones podemos concluir que el bien jurídico tutelado en estos artículos es la indemnidad del menor, por lo cual debemos precisar que en el caso de los montajes de fotografías de menores en un contexto pornográfico no caería dentro de la norma.

2.2 Producción y difusión de pornografía Infantil motivada por el auge de Internet.

El tema de la pornografía infantil tiene, en sus inicios, un carácter internacional y comercial. Se produce material de pornografía infantil con un ánimo de lucro.[149] La aparición de Internet produce algunos cambios, los que se traducen en una transformación de la dinámica de producción y comercialización que a continuación explicaremos.

La tecnología digital reduce los costos de producción de material, lo que permite a una mayor cantidad de personas producir pornografía infantil. Ello, unido a la facilidad que proporciona Internet para la distribución, hace que el fin comercial y el ánimo de lucro, se desvanezca. Fermín Morales lo expresa en términos que "*puede trazarse una línea evolutiva que desplaza la elaboración y producción de la pornografía infantil de parámetros comerciales organizados a ámbitos descentralizados amateurs y domésticos. Cualquier usuario de la Red tiene acceso a los servicios en línea en una autopista de información a la que se encuentran conectados más de 30 millones de personas. En este contexto, cualquier usuario puede erigirse en productor, difusor o receptor de material pornográfico infantil"*[150].

[149] Ibíd.

[150] "En la actualidad se constata una tendencia según la cual el tráfico de pornografía infantil no viene presidido por el ánimo de lucro ni por motivos comerciales. Se ha acrecentado así el intercambio de

Uno de los problemas para la investigación de estos delitos es que la difusión y tráfico de pornografía infantil puede ser llevada a cabo desde el anonimato que proporciona Internet. Así las dificultades que se presentan son:

A) Los usuarios no señalan su verdadera identidad, ocupan apodos.

Así se señaló en la discusión en el Congreso de la ley 19.927 que "*el mayor problema que se presenta para individualizar a las personas correspondientes a los "nick names". Sería relevante contar con medios legales que permitieran a la policía disponer de "herramientas" tales como agentes encubiertos, interceptación de comunicaciones y compras simuladas de material pornográfico, a fin de desbaratar de la manera más diligente y oportuna a las organizaciones que cometen este tipo de delitos"* [151].

B) Determinación del origen de los contenidos.

De igual manera en el Congreso sobre este punto se señaló que "*resultaría oportuno la creación de normas legales que permitan obtener información rápida y certera por parte de las empresas telefónicas, fijando plazos para ello, tendientes a ubicar la dirección IP de los computadores, que es el número asociado matemáticamente a un computador de características únicas. Si las compañías*

material entre pedófilos, pauta de comportamiento que se ha amplificado en las nuevas autopistas de la información (Internet), donde los usuarios pueden introducir material y convertirse en difusores de dicho material".MORALES, Fermín, p.4.

[151] Opinión de la Jueza Verónica Sabaj en INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO recaído en el proyecto de ley, en segundo trámite constitucional, que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal, en materias de delitos de pornografía infantil. BOLETÍN N° 2906-07

telefónicas o los servidores no entregan la información dentro de un plazo determinado, la investigación se hace ilusoria".[152]

Hay que tener en consideración el hecho que también existen diversas maneras de evitar el conocimiento del origen del material pornográfico. Un caso es el uso de los *anonymous remailers*, que permiten el envío de correos electrónicos sin remitente; "*los remailers suponen el uso de servidores de correo electrónico intermedios entre el remitente y el destinatario final, de modo que el remitente envía un mensaje a un servidor que, a la vez, lo reenvía al destinatario final sin que aparezcan los datos del remitente*"[153].

Para luchar contra la pornografía infantil se han realizado una serie de reuniones de expertos, siendo una la que marca una pauta debido, a las conclusiones y sugerencias que se entregan. Esta es la celebrada en Lyon entre el 28-29 de mayo de 1998 que plantea la necesidad de adoptar leyes que incriminen la producción, distribución, importación, exportación y posesión de pornografía infantil [154].

---

[152] INFORME DE LA COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN, JUSTICIA Y REGLAMENTO recaído en el proyecto de ley, en segundo trámite constitucional, que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal, en materias de delitos de pornografía infantil. BOLETÍN N° 2906-07

[153] MORALES, Fermin. Op. Cit. p.3

[154] Las recomendaciones son: a) La necesidad de adopción en la legislación de los ordenamientos nacionales de medidas legislativas que incriminen la producción, distribución, comunicación, importación, exportación y posesión de pornografía infantil, incluida la pseudopornografía, a través de Internet. b)La armonización internacional en cuanto al límite de edad en la conceptualización de los menores y en cuanto a la definición de pornografía infantil; c) El incremento de la cooperación policial y judicial, tanto en cuestiones relativas a la aplicación de la ley penal como con relación a la asistencia técnica; d) La solicitud a las Naciones Unidas de que impulse un borrador de legislación tipo, uniforme, contra la pornografía infantil; e)La solicitud al Comité sobre Derechos de los Niños de las Naciones Unidas de que impulse la aplicación de controles legales adecuados contra la pornografía infantil, cuando los gobiernos presenten sus informes nacionales en la Convención sobre Derechos del Niño; f) La promoción del desarrollo de programas similares a los antivirus, que permitan filtrar o bloquear la pornografía infantil en Internet, a través de los proveedores de servicio en Internet (PSI), mediante una base de datos central actualizada regularmente con impresiones de imágenes de pornografía infantil.
Prevención de la pornografía infantil en la Internet, http://www.ecpat.net/es/Ecpat_inter/projects/preventing_pornography/prevent.asp, última visita 4 de Agosto 2006.

En tanto, la Brigada del Cibercrimen de la Policía de Investigaciones señala que sería de utilidad establecer el agente encubierto, el registro nacional de rangos de IP del proveedor; la tramitación con los ISP; el tiempo de almacenamiento del registro de IP, la incautación de los medios y la tecnología utilizada; y conocer los códigos fuente de las páginas web. Además de plantear la posibilidad de facultar a los tribunales para conocer de aquellas conductas que, aún cuando no se han realizado en el país -lo que puede ocurrir con internet-, surten efectos en él. Sobre el particular precisaron que, en la mayoría de las situaciones, debe recurrirse a la cooperación internacional, que no es prestada en forma homogénea por los distintos[155].

La llamada ley de Pornografía Infantil en cuanto modifica el Código Penal señala en el artículo 374 bis : *"El que comercialice, importe, exporte, distribuya, difunda o exhiba material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será sancionado con la pena de presidio menor en su grado medio a máximo. El que maliciosamente adquiera o almacene material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será castigado con presidio menor en su grado medio."*

La controversia surge con la incriminación de la tenencia de material pornográfico —inciso 2º 374 bis—. La idea del legislador al comprender en el tipo al usuario, es que la cadena pornográfica termina en él. Son éstos los que, en definitiva, le dan sentido a la existencia del material. El legislador estima que castigando a la demanda se termina con la oferta.

[155] Informe de la comisión de Constitución, Legislación, Justicia y reglamento recaído en el proyecto de ley, en segundo trámite constitucional, que modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal, en materias de delitos de pornografía infantil. BOLETÍN N° 2906-07.

El Convenio Sobre la Ciberdelincuencia hace referencia a lo que se debería tipificar como delito. Así se señala[156]: "Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; c) la difusión o transmisión de pornografía infantil por medio de un sistema informático, d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos."

En vista de los problemas conceptuales sobre qué debe entenderse por pornografía infantil el Convenio mismo lo expresa:

"Por pornografía infantil se entenderá todo material pornográfico que contenga la representación visual de:

a) Un menor comportándose de una forma sexualmente explícita;

b) Una persona que parezca un menor comportándose de una forma sexualmente explícita;

c) Imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita".[157]

El Convenio plantea el hecho de incriminar la posesión de material de pornografía infantil. Además, la delimitación conceptual de pornografía infantil incluye lo que es la pornografía Técnica (una persona que parezca un menor comportándose de

[156] Convenio sobre la Ciberdelicuencia, Título 3 del Capítulo II, sección 1, Derecho penal sustantivo, sobre delitos relacionados con el contenido, artículo 9.

[157] Convenio sobre la Ciberdelicuencia, Título 3 del Capítulo II, sección 2, Derecho penal sustantivo, sobre delitos relacionados con el contenido, artículo 9.

una forma sexualmente explícita) y la pseudopornografía (imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita).

Los Estados partes pueden reservase el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado1, esto es la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona y la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. Lo mismo cabe respecto a las letras b y c del apartado 2 que corresponde a la pornografía infantil técnica y la pseudopornografía.

En estos casos de posesión de material de pornografía infantil pueden presentarse dudas para el ISP en cuanto a que actitud adoptar ante la posible existencia de un delito. En primer lugar, normativamente los ISP tienen deberes de registro que ante la exigencia de los organismos competentes deben facilitar para poder perseguir los delitos. En definitiva estos deberes se traducen en colaboración con los organismos competentes, de lo cual no se podría derivar que los ISP tengan deberes de cuidado en cuanto a los posibles delitos que se pusieran cometer, los ISP no se pueden convertir ni normativa ni fácticamente en vigilantes.

La palabra *"almacene"* debe entenderse que incluye sólo a quienes tengan en su poder un material cuantioso. En efecto, la expresión almacenar, significa reunir o guardar muchas cosas[158]. Por tanto, se refiere a aquellos sujetos que cuenten con suficiente material que permita sostener que pretende comercializarlo o distribuirlo.

Existe una opinión del debate parlamentario del Senador Naranjo que expresa *"si hay pornografía infantil actualmente es porque existe, repito, un mercado exigente que la demanda. Mientras más pequeños son los menores, más dinero se paga"*[159]. Esta

[158] Diccionario de la Real Academia de la Lengua Española, 22 ª edición, año 2001, p.115
[159] Diario de sesiones del Senado Publicación Oficial Legislatura 350ª, Extraordinaria Sesión 2ª, en miércoles 8 de octubre de 2003 Ordinaria p.60.

opinión no toma en consideración la línea evolutiva que ha tenido la pornografía infantil, en cuanto ya no es claramente distinguible el fin comercial o de lucro, el gran problema hoy es el intercambio.

Hay que tener presente "*los peligros de esta suerte de neointegrismo punitivo., Las opciones irracionalmente incriminadoras deben ser descartadas; en esta dirección apuntan las propuestas de intervención del Derecho Penal, cifradas en operar sobre la demanda de material pornográfico infantil como medio para poner coto a la oferta, lo que implica la criminalización de la mera tenencia,* que no dan resultado práctico"[160].

Para nuestra tesis resulta importante presenciar como cada vez de forma más habitual, el anonimato se relaciona con conductas ilegales. El anonimato no es la fuente de la ilicitud en Internet. Los partidarios del anonimato no son potenciales delincuentes, sino sujetos que lo consideran como una garantía esencial.

3. Registro de Datos de Tráfico y su relación con el Tráfico de llamadas Telefónicas.

La ley 19.927 modificó el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal. En lo que nos atañe, estableció deberes de Registro a los ISP, estos se encuentran en el Código Procesal Penal, en el Artículo 222 inciso 4º, que señala lo siguiente: "Las empresas telefónicas y de telecomunicaciones deberán otorgar a los funcionarios encargados de la diligencia las facilidades necesarias para llevarla a cabo, **en el menor plazo posible. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a seis meses, de los números IP de las conexiones que realicen sus abonados**. La negativa o entorpecimiento a la práctica de la medida de interceptación y

[160] MORALES, Fermín, Op. Cit. p.10.

grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento". (En negritas la modificación)[161].

Para poder analizar este artículo debemos precisar qué se entiende por datos de tráfico, teniendo como primer punto de referencia lo señalado en la legislación comparada.

Un primer concepto lo encontramos en el Convenio Sobre la Ciberdelincuencia que señala en su Artículo 1 d): "Por datos sobre el tráfico se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático,

[161] Texto completo del artículo 222 del Código Procesal Penal señala: "Articulo 222: Interceptación de comunicaciones telefónicas. Cuando existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión, o que ella preparare actualmente la comisión o participación en un hecho punible que mereciere pena de crimen, y la investigación lo hiciere imprescindible, el juez de garantía, a petición del ministerio público, podrá ordenar la interceptación y grabación de sus comunicaciones telefónicas o de otras formas de telecomunicación.

La orden, a que se refiere el inciso precedente, sólo podrá afectar al imputado o a personas respecto de las cuales existieren sospechas fundadas, basadas en hechos determinados, de que ellas sirven de intermediarias de dichas comunicaciones y, asimismo, de aquellas que facilitaren sus medios de comunicación al imputado o sus intermediarios.

No se podrán interceptar las comunicaciones entre el imputado y su abogado, a menos que el juez de garantía lo ordenare, por estimar fundadamente, sobre la base de antecedentes de los que dejará constancia en la respectiva resolución, que el abogado pudiere tener responsabilidad penal en los hechos investigados. La orden que dispusiere la interceptación y grabación deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar la forma de la interceptación y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por períodos de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

Las empresas telefónicas y de telecomunicaciones deberán otorgar a los funcionarios encargados de la diligencia las facilidades necesarias para llevarla a cabo, en el menor plazo posible. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a seis meses, de los números IP de las conexiones que realicen sus abonados. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento

Si las sospechas tenidas en consideración para ordenar la medida se disiparen o hubiere transcurrido el plazo de duración fijado para la misma, ella deberá ser interrumpida inmediatamente".

generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el orígen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente".

En tanto, la Directiva Europea sobre la Privacidad y las Comunicaciones Electrónicas señala en su Artículo 2 b) :"Datos de tráfico es cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma".

Importante es mencionar al respecto lo que se entiende por comunicaciones, siendo esta señalada en la letra d) del artículo 2, de la mencionada directiva, que define comunicación como *"cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información"* [162].

Un problema procesal se ha planteado en torno al registro de datos que poseen las empresas telefónicas. Situación que es aplicable tanto a los registros de llamadas telefónicas, como a los registro de los números IP autorizados, que señala el artículo 222 de Código Procesal Penal. Por lo general, en investigaciones sobre tráfico de drogas, una de las diligencias que se realiza es solicitar a la empresa telefónica o de telecomunicaciones, la remisión de un registro o listado de las llamadas telefónicas entrantes y salientes de una línea telefónica.

[162] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de las Comunidades Europeas.* 31 Julio de 2002.

Ante esta situación una posición jurídica estima que se debe exigir a los fiscales la autorización por el juez de garantía para proceder a la entrega de los registros de datos de tráfico de llamadas, en virtud de lo dispuesto en los artículos 9 y 219 de Código Procesal Penal[163]. Esto por cuanto la solicitud de entrega de dichos registros podría afectar la garantía constitucional contemplada en el Artículo 19 Nº 4 de la Constitución.

Las empresas de telecomunicaciones tienen razones para argumentar que es necesario la autorización del juez de garantía. Se basan en que debe efectuarse una interpretación armónica de los artículos anteriormente señalados.

Frente a la postura anterior, existe otra representada por el Ministerio Público que señala al respecto que "*la exigencia de autorización previa, sin perjuicio de retardar la persecución penal, implica extender la cautela de garantías hasta límites insospechados por el legislador, olvidando que toda actividad de persecución penal siempre implica inevitablemente por sí misma, la afectación de algunas garantías, y como primera de ellas, la intimidad de todo inculpado"*[164].

Lo que plantea el Ministerio Público es aplicar una interpretación sistemática del Código Procesal Penal, específicamente de las normas sobre diligencias intrusivas y sobre las facultades autónomas de actuación de las policías. Luego de esto, el argumento

---

[163] El artículo 9º trata sobre la autorización Judicial Previa. Dicho artículo señala:"Autorización judicial previa. Toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa.
En consecuencia, cuando una diligencia de investigación pudiere producir alguno de tales efectos, el fiscal deberá solicitar previamente autorización al juez de garantía.
Tratándose de casos urgentes, en que la inmediata autorización fuere indispensable para el éxito de la diligencia, podrá ser solicitada y otorgada por cualquier medio idóneo al efecto, tales como teléfono, fax, correo electrónico u otro, sin perjuicio de la constancia posterior."
En tanto el Artículo 219 trata sobre las copias de comunicaciones y transmisiones, en donde el juez de garantía puede autorizar la facilitación de copias a petición del fiscal.
Artículo 219.- Copias de comunicaciones o transmisiones. El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa de comunicaciones facilite copias de las comunicaciones transmitidas o recibidas por ellas. Del mismo modo, podrá ordenar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios.

[164] RETAMAL, Jaime, Boletín del Ministerio Público, N° 20, Septiembre 2004., p.153,

es que la petición de entrega del listado o registro de datos sobre llamadas tiene el carácter de requerimiento de información y entonces es aplicable el artículo 180 del Código Procesal Penal[165], con lo cual no es necesaria la autorización de la diligencia por parte del juez de garantía.

La fundamentación es que la petición de los datos de registro es un requerimiento de información. La interpretación que se le debe dar al artículo 9 º, de acuerdo al Ministerio Público, es la de una norma de clausura que sólo cobra vigencia cuando se afecte una garantía fundamental de manera relevante, por la actividad investigativa, siendo necesario en estos casos, recabar autorización judicial en forma previa a la actuación.

El legislador reguló las medidas intrusivas de común ocurrencia en la fase investigativa y que afecten garantías constitucionales. El Código Procesal Penal regula los exámenes corporales, pruebas caligráficas, incautación de objetos y documentos e interceptación de comunicaciones.

El Código Procesal Penal autoriza a que algunas diligencias que afectan garantías constitucionales se realicen sin autorización judicial previa. En este caso es la propia ley la que autoriza. Los ejemplos que se dan al respecto son el control de identidad (art. 85), la detención por flagrancia (art. 130), las facultades autónomas de la policía (art. 83), y las facultades de investigación propias de los fiscales (art. 180 y 181). Así el ámbito de

[165] El Artículo 180 del Código Procesal Penal señala: "Investigación de los fiscales. Los fiscales dirigirán la investigación y podrán realizar por sí mismos o encomendar a la policía todas las diligencias de investigación que consideraren conducentes al esclarecimiento de los hechos.

Sin perjuicio de lo dispuesto en el Párrafo 1º de este Título, dentro de las veinticuatro horas siguientes a que tomare conocimiento de la existencia de un hecho que revistiere caracteres de delito de acción penal pública por alguno de los medios previstos en la ley, el fiscal deberá proceder a la práctica de todas aquellas diligencias pertinentes y útiles al esclarecimiento y averiguación del mismo, de las circunstancias relevantes para la aplicación de la ley penal, de los partícipes del hecho y de las circunstancias que sirvieren para verificar su responsabilidad. Asimismo, deberá impedir que el hecho denunciado produzca consecuencias ulteriores.

Los fiscales podrán exigir información de toda persona o funcionario público, los que no podrán excusarse de proporcionarla, salvo en los casos expresamente exceptuados por la ley."

aplicación está dado por la ausencia de regulación expresa de la medida intrusiva y por la afectación de una garantía constitucional en una entidad suficiente que justifique la intervención jurisdiccional.

La posición del Ministerio Público es que "*la aplicación del artículo 9º exige que la afectación del derecho constitucional sea precisamente mediante su privación, restricción o perturbación, y que ella sea ponderada por el juez de garantía, como de similar entidad o gravedad que las situaciones reguladas expresamente por las diligencias intrusivas, ya que de otro modo, la más mínima e incluso irrelevante afectación de una garantía motivaría la intervención del aparato jurisdiccional, lo que resulta innecesario y excesivo, ya que siempre está latente como contrapartida el legítimo interés en la persecución penal*[166].

Siguiendo el argumento del Ministerio Público, la entrega de información sobre el tráfico no puede significar privar o restringir la vida privada e intimidad. Si bien puede haber perturbación, ella no es comparable a las demás medidas intrusivas reguladas específicamente en el Código. Ante una mínima afectación no resulta necesaria la autorización judicial previa.

El segundo punto del argumento del Ministerio Público es que la petición de los registros no es más que un requerimiento de información a la que esta facultado el fiscal de acuerdo al artículo 180 en su inciso final[167].

Las empresas de telecomunicaciones de permitírseles no entregar la información ante el requerimiento del fiscal estarían en una situación de privilegio frente a la comunidad.[168]

---

[166] RETAMAL, Jaime, Op. cit. p.155

[167] *Un registro de llamadas entrantes y salientes, no deja de ser un requerimiento particular de información, por mucha proximidad que tenga con la existencia de una comunicación privada, y su afectación no tiene ni tendrá jamás la misma entidad que la interceptación y grabación de conversaciones,"* RETAMAL, Jaime, p.155.

Existiría el absurdo que (de aceptarse que deban pedir autorización para que se les entreguen los datos de tráfico), deberían pedir autorización del juez para requerir todo tipo de información. Con lo cual *"carece de realismo y practicidad, que el más mínimo requerimiento de información obligue a un pronunciamiento jurisdiccional previo, y de esta forma, el registro de llamadas de una línea telefónica no puede ser la excepción, ya que por lo demás no tiene el carácter invasivo de la intercepción, registro o escucha, propios de la interceptación. De aceptarse la tesis jurídica que se impugna, todo requerimiento de información, sin excepción, debiera ser cursado por el juez de garantía mediante su autorización, lo que además de ser impracticable, llevaría a algunas situaciones de absurdo"*[169].

Con respecto a la confidencialidad de las comunicaciones, el planteamiento es que las empresas ante el requerimiento de la fiscalía entreguen la información por cuanto sus clientes están resguardados en virtud del artículo 182 del Código Procesal Penal que trata del secreto de las actuaciones[170].

---

[168] Ibíd. p.155.

[169] RETAMAL, Jaime, Op. cit. p.156

[170] artículo 182 del Código Procesal Penal: Secreto de las actuaciones "Las actuaciones de investigación realizadas por el ministerio público y por la policía serán secretas para los terceros ajenos al procedimiento.

El imputado y los demás intervinientes en el procedimiento podrán examinar los registros y los documentos de la investigación fiscal y policial.

El fiscal podrá disponer que determinadas actuaciones, registros o documentos sean mantenidas en secreto respecto del imputado o de los demás intervinientes, cuando lo considerare necesario para la eficacia de la investigación. En tal caso deberá identificar las piezas o actuaciones respectivas, de modo que no se vulnere la reserva y fijar un plazo no superior a cuarenta días para la mantención del secreto.

El imputado o cualquier otro interviniente podrán solicitar del juez de garantía que ponga término al secreto o que lo limite, en cuanto a su duración, a las piezas o actuaciones abarcadas por él, o a las personas a quienes afectare.

Sin perjuicio de lo dispuesto en los incisos anteriores, no se podrá decretar el secreto sobre la declaración del imputado o cualquier otra actuación en que hubiere intervenido o tenido derecho a intervenir, las actuaciones en las que participare el tribunal, ni los informes evacuados por peritos, respecto del propio imputado o de su defensor.

Los funcionarios que hubieren participado en la investigación y las demás personas que, por cualquier motivo, tuvieren conocimiento de las actuaciones de la investigación estarán obligados a guardar secreto respecto de ellas".

Por último, el criterio de actuación es que en casos urgentes puede resultar más práctico requerir directamente la información acudiendo previamente ante el juez de garantía, esa sería la excepción[171].

Frente a este planteamiento hay que hacer los siguientes comentarios.

1- La tesis descrita hace una diferenciación tajante entre lo que son datos de tráfico y lo que es el contenido de las comunicaciones, en donde el primero da la impresión de no tener la relevancia del segundo.

El derecho a la confidencialidad de las comunicaciones sólo protegería el contenido de éstas. Sin embargo, existe una tendencia que consiste en brindar protección tanto al contenido de las comunicaciones como a los datos de tráfico. No existe una diferencia tajante al respecto.

Para ejemplificar lo anterior, en la normativa europea se plantea en el artículo 5 de la directiva 2002/58 sobre la privacidad y las comunicaciones electrónicas que la confidencialidad de las comunicaciones incluye los datos de tráfico asociados a ella. El texto expreso señala lo siguiente:

> "Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de la

[171] RETAMAL, Jaime, Op. cit. p.156

comunicación, sin perjuicio del principio de confidencialidad"[172]. (subrayado nuestro)

2- El concepto de intimidad, en el planteamiento del Ministerio Público, se vincula con un espacio físico o con el contenido de las comunicaciones. Señala que "*la intimidad como garantía constitucional parece vincularse con un espacio físico de un individuo o con el contenido de sus comunicaciones, lo que deben desenvolverse sin intervención o presencia de terceros"*[173].

El concepto que se da de intimidad (por parte del Ministerio Público) es restringido. Bajo ese prisma se entiende que se separen lo que es el contenido de la comunicación de los datos asociados a ella.

Desde una perspectiva subjetiva, la intimidad puede ser concebida como autodeterminación informativa, esto es como la facultad del individuo, grupo o institución de determinar por sí mismo cuándo, cómo y en que grado puede comunicarse a otros información sobre él[174]. Bajo esa mirada los datos como el contenido de la comunicación están asociados.

En todo acto de comunicación hay un mensaje con un contenido intelectual determinado. Existe un proceso de transferencia del mensaje a través de algún medio técnico y hay unos datos relativos al proceso mismo de comunicación, que sin formar parte del contenido intelectual del mensaje, son indisociables de la realidad misma de la comunicación.

---

[172] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de las Comunidades Europeas.* 31 Julio de 2002

[173] RETAMAL, Jaime, Op. cit. p.154

[174] HORVITZ, María Inés , LOPEZ, Julian p.521. Además señalan que "*este derecho determina una facultad de exclusión de los demás, de abstención de injerencias por parte de otros, tanto en lo que se refiere a la adquisición del conocimiento ajeno como a su divulgación".*

3- En relación con el ciberespacio se presentan tensiones por los derechos que existen en la red. Se consolida la idea que las reglas en la Red no pueden quedar al albur exclusivo de los usuarios. El magma de intereses contrapuestos en Internet (derecho al anonimato del usuario, garantía de la confidencialidad de comunicaciones personales en la Red, confianza y seguridad jurídica en el mercado virtual, preservación de la seguridad y defensa de los Estados) exige nuevas soluciones jurídicas complejas, que atiendan al principio de proporcionalidad, en el buen entendido de que se trata mediante el mismo de garantizar la convivencia y preservación simultánea de intereses legítimos en tensión.

Se deben descartar soluciones simplistas que superen las esquemáticas dicotomías "liberalización contra control" o "estados contra usuarios"[175]. En lo que hemos analizado, existe una dicotomía entre Ministerio Público y Empresas de telecomunicaciones, que hay que superar.

En España se produjo una discusión en términos similares a los expresados en las líneas anteriores. Nos parece atinente explicitarlo para la compresión del hecho y su solución.

El hecho que motiva la discusión es la investigación sobre un delito cometido contra una empresa informática. Una empresa de sistemas informáticos sufre un acceso indebido a sus computadores por parte de personas no identificadas. Estos provocan el borrado de diversos ficheros. La investigación e instrucción de la causa requiere en estos casos como primera diligencia la identificación de los abonados desde cuyos teléfonos o terminales se han realizado las conexiones, lo que obliga a acudir al operador del servicio telefónico para recabar la información correspondiente.

El Fiscal solicita al operador telefónico el conocimiento de los números de abonado desde los que se verificaron las conexiones. La compañía operadora entiende

[175] MORALES, Fermín, Op. cit p.20.

que la información solicitada afecta al estatuto constitucional de inviolabilidad de las comunicaciones -art. 18.3 CE- y deniega el acceso a los datos en tanto no sea autorizada por una resolución judicial[176].

Esta postura implica una restricción de las facultades de investigación del Fiscal. En la medida en que el artículo 5.2 del Estatuto Orgánico reduce la legitimación para la adopción de medidas de investigación a aquellas que no sean limitativas de derechos, por lo que la selección del régimen constitucional de garantía que le cuadra a este tipo de datos y contenidos, sea el estatuto de inviolabilidad del artículo 18.3 de la Constitución Española, sea la libertad informática del artículo 18.4 Constitución Española, repercute de inmediato en la afirmación de la existencia o inexistencia de posibilidades de investigación autónoma por parte del Ministerio Fiscal.[177]

La opinión de la fiscalía es que sólo la interceptación del contenido exige autorización judicial, lo que a contrario sensu conduce a estimar no abarcado en el secreto de las comunicaciones los aspectos e informaciones no comprendidos en el contenido mismo[178].

---

[176] Artículo 18.3 Constitución Española**. "**Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial." 18.4. "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

[177] Artículo 5 del Estatuto Orgánico**:** El Fiscal podrá recibir denuncias, enviándolas a la autoridad judicial o decretando su archivo cuando no encuentre fundamentos para ejercitar acción alguna, notificando en este último caso la decisión al denunciante.
Igualmente, y para el esclarecimiento de los hechos denunciados o que aparezcan en los atestados de los que conozca, puede llevar a cabo u ordenar aquellas diligencias para las que este legitimado según la Ley de Enjuiciamiento Criminal, las cuales no podrán suponer, adopción de medidas cautelares o limitativas de derechos. No obstante, podrá ordenar el Fiscal la detención preventiva.
Todas las diligencias que el Ministerio Fiscal practique o que se lleven a cabo bajo su dirección, gozarán de presunción de autenticidad.

[178] La Fiscalía estima que el estatuto de inviolabilidad sólo opera cuando el acto de comunicación es interceptado en tiempo real, esto es, mientras se produce la transferencia del mensaje, pues considera que el bien protegido es el libre flujo de las comunicaciones, de modo que extinguida la comunicación, los datos que se registran en soporte informático para la facturación del servicio prestado quedarían sujetos al régimen específico del artículo 18.4 Constitución Española que no exige habilitación judicial para la cesión de información en favor del Ministerio Fiscal.

La conclusión a que se llega luego del debate es que exigir del operador telefónico la identificación de los números de abonado conectados en una concreta y determinada comunicación supone una restricción de derechos prohibida por la legislación española. Es preciso acudir al Juez de Instrucción, justificar la necesidad de la medida.

Las diligencias de investigación preprocesal amparadas en los artículos 5° del estatuto orgánico ministerio fiscal y las posibilidades de investigación autónoma para-procesal no constituyen un marco legal idóneo para exigir del operador de la red o del prestador del servicio la revelación de los datos de tráfico registrados en las comunicaciones establecidas.

El proceso de comunicación y el mensaje son el continente y el contenido de una misma realidad y constituyen aspectos tan indisociables desde el punto de vista material que merecen, en línea de principio, un tratamiento jurídico homogéneo.

La doctrina del Tribunal Europeo de Derechos Humanos ha delimitado con la extensión material de este derecho fundamental. Destaca la Sentencia del Tribunal de Estrasburgo dictada en el caso Malone el día 2 de agosto de 1984 en cuanto declara categóricamente, en relación con las comunicaciones telefónicas, el registro que por legítimos fines comerciales verifica el titular del servicio mediante un contador de los números que han sido marcados desde un determinado aparato suministra una información de la que no se puede hacer uso sin la previa autorización del afectado[179].

[179] La Sentencia del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984, caso *Malone c. Reino Unido*, se pronunció sobre la afectación del derecho reconocido en el art. 8.1 del Convenio europeo de derechos humanos por el sistema denominado *comptage* —sistema electrónico del que se sirven las empresas de comunicación para relacionar y facturar las llamadas de sus clientes— a pesar de que este mecanismo sólo registra los números marcados y no suponen la interceptación de las conversaciones telefónicas. En dicha Sentencia se afirma expresamente que en los listados figuran informaciones que son parte integrante de las comunicaciones telefónicas, en particular, los números de destino de las llamadas. Lo que indica la doctrina del Tribunal de Estrasburgo es que no se pueden disociar sin merma relevante de garantías realidades tan sustancialmente integradas como son el mensaje y su proceso de transmisión.

Desde esta perspectiva es claro que inviolable no sólo es el mensaje, sino todos aquellos datos relativos a la comunicación que permitan identificar a los interlocutores o corresponsales, o constatar la existencia misma de la comunicación, su data, duración y todas las demás circunstancias concurrentes útiles para ubicar en el espacio y en el tiempo el hecho concreto de la conexión telemática producida.

La Constitución protege no sólo el proceso de comunicación, sino también el mensaje, en el caso de que éste se materialice en algún objeto físico, y el objeto del secreto abarca no sólo el contenido de la comunicación sino también otros aspectos de la misma como por ejemplo la identidad subjetiva de los interlocutores o corresponsales[180].

4. Propiedad Intelectual en la Red y como afecta la Privacidad.

La importancia de analizar el impacto de Internet en la propiedad intelectual, para objeto de determinar como se ve afectada la privacidad, dice relación con una tendencia a criminalizar ciertos actos en la red, como el intercambio de contenidos a través de redes de p2p. Al criminalizar a una gran cantidad de gente se producen daños colaterales para las libertades públicas, en este caso se produce una pérdida de privacidad por parte de los usuarios. Para analizar los alcances y experiencias acerca de este fenómeno, estudiaremos los casos de Estados Unidos, el TLC de este país con Chile, y algunas ideas matrices de directivas Europeas. Para ello, comencemos con una primera aproximación a la criminalización de los actos en la red.

Lessig lo explica citando a Von Lohmann expresando que "*Si puedes tratar a alguien como a un presunto delincuente", entonces de repente muchas protecciones básicas de las libertades civiles se evaporan en un grado u otro. [...] Si violas el copyright, ¿cómo puedes esperar cualquier derecho a la intimidad? Si violas el*

[180] Circular número 1/1999, 29 de Diciembre de 1999, sobre la intervención de las comunicaciones telefónicas en el seno de los procesos penales, http://www.mju.es/guia_fiscalia.htm , (última visita 4 de Junio 2005).

copyright, ¿cómo puedes esperar tener la seguridad de que no van a decomisar tu computadora? [...] Nuestros sentimientos cambian en cuanto pensamos: "Ah, bueno, pero esa persona es un delincuente, un criminal". Bueno, lo que esta campaña contra el intercambio de ficheros ha conseguido es convertir en "delincuentes" a un porcentaje notable de la población de los internautas"[181].

La tecnología p2p implica el intercambio de ficheros entre iguales (p2p sigla en inglés) es una tecnologías que facilita la difusión de contenidos de una forma que nadie habría imaginado hace una generación.

Una red p2p se basa principalmente en la filosofía de que todos los usuarios deben compartir. Tiene un carácter meritocrático, ya que el que más comparte, más privilegios tiene y dispone de manera más rápida a mayores contenido. Con este sistema se pretende asegurar la disponibilidad del contenido compartido.

Los usuarios de estas redes lo utilizan para los siguientes usos: sustituto de la compra de CDs, escuchar partes de los mismos antes de comprarlos, uso de las redes para acceder a contenido de difícil de encontrar, y también para acceder a contenidos de dominio público sin las restricciones de la propiedad intelectual[182]. *"El "problema" con el intercambio de archivos--en la medida en la que hay un problema real--es un problema que irá desapareciendo conforme sea más fácil conectarse a Internet"*[183], luego en la medida que el ancho de banda aumente, ya no será conveniente estar almacenando los contenidos que se descargan.

Con las ideas anteriores, ya podemos explicar como opera la criminalización y persecución. Tomemos como parámetro EE.UU. La RIAA, corresponde a la asociación americana de industrias de la música[184], que es la entidad que presenta demandas[185]

[181] LESSIG, Lawrance, "Cultura libre", Op.cit. pp. 229-230.
182 Ibíd. p. 329.
183 Ibíd. p. 331.
[184] Record Industry American Asociation, RIAA, por sus siglas en inglés.

contra los usuarios de las redes p2p que comparten contenidos. La identidad de los usuarios se desconoce y tan sólo dispone de las direcciones IP. Para averiguar las identidades de los usuarios debe lograr que los proveedores de servicios de Internet se los entreguen, para ello se inician procesos judiciales. En el año 2000, RIAA lanzó una campaña para forzar a los proveedores de Internet a entregar los nombres de los clientes que pensaba que estaban violando la leyes de propiedad intelectual. Según los estudios más conservadores, 60 millones de estadounidenses utilizan esta tecnología. Es de esta manera que 60 millones de personas son consideradas potenciales delincuentes. Las cifras de usuarios de estas redes deben ser extrapoladas a nivel mundial. Es tanta la presión a los ISP que estos terminan por colaborar con la RIAA.

Napster, que fue el iniciador de estas redes, y alcanzó gran popularidad se convirtió, luego de un largo proceso judicial, en un catálogo de música online pagado.

El juicio contra Napster[186] se desarrolló en los siguientes términos: Napster proporcionaba gratuitamente un software para que los usuarios se pusieran en contacto entre ellos, identificaran qué grabaciones tenía cada uno y se las intercambiaran entre sí. Los miembros de la comunidad no tenían que demostrar haber comprado un CD original. Napster no mantenía una base de datos con los materiales de sus suscriptores; de hecho, no había una base de datos central, ni tampoco había suscripciones. Bajo la ley de Propiedad Intelectual norteamericana, (USCA)[187], la responsabilidad vicaria dependía de que existiera infracción por parte de sus usuarios, que hacían copias de las grabaciones de otros, y ponían sus propias grabaciones a la disposición de los restantes

[185] En un año, la RIAA ha denunciado ya a 5.400 personas por este mismo motivo, a la fecha 10-10-2004. Entre los demandados hay estudiantes de 26 colegios y universidades. Presionadas por la RIAA –que representa a las principales discográficas del mundo, como Warner Music, EMI Bertelsmann, Sony y Vivendi Universal–, muchas universidades han tomado medidas para limitar el intercambio de archivos concediendo http://www.libertaddigital.com/noticias/noticia_1276234135.html, (última visita 20 de Junio 2005)

[186] Sentencia en caso de A&M Records contra Napster, 239 F. 3d 1004 9th Cir., de 12 de febrero de 2001, en http://www.usdoj.gov/criminal/cybercrime/napsterbr.htm (última visita 15 de Junio 2005)

[187] United States Copyright Act of 1976, corresponde a la ley de Propiedad Intelectual previa a la Digital Millennium.

miembros. El tribunal realizó el siguiente análisis : "Los usuarios consiguen gratis algo que de ordinario deberían comprar", por lo que las grabaciones realizadas por los usuarios tiene carácter "comercial" y no pueden quedar cubiertas por la doctrina del *fair use*. Así, declaró que era responsable por infracción de la propiedad intelectual. En consecuencia, ordenó que si quería evitar ser considerado responsable debía realizar filtrado de los contenidos que se transmitían a través de su software, para identificar y retirar las de los demandantes [188].

En la práctica, tuvo que cerrar hasta desarrollar un sistema que le permita controlar los contenidos. Paralelamente al litigio, llegó a un acuerdo con la mayoría de empresas discográficas para establecer cuotas de remuneración por las copias realizadas a través de su software; Napster reabrió, pero los usuarios deben pagar. Con el tiempo se han creado más sistemas para compartir archivos. Algunos de ellos, son más sofisticados al no existir ni tan siquiera un "proveedor" del software a quien demandar y responsabilizar.[189] Así es como, dentro del catalogo de Napster, las canciones en formato mp3 poseen un huella digital que permite que cada copia que se haya realizado de la misma canción posea una identificación. Esto permite que sean pesquisables las copias que se hayan realizado violando la propiedad intelectual[190].

Como es lógico a los usuarios los protege la presunción de inocencia. Esta presunción de inocencia se desvanece porque el Derecho a defensa se presenta como una ilusión; solo existe si el usuario puede costearse los servicios de un abogado. Es en ese aspecto en donde entra a jugar el tema de la intimidación a los usuarios, a los ISP, a las

[188] XALABARDER, Raquel, "Infracciones de propiedad intelectual y la Digital Millennium Copyright Act", 2002, http://www.uoc.edu/in3/dt/20060/index.html, última visita 15 Junio 2005.
[189] Información en el sitio de Electronic Frontier Foundation, http://www.eff.org , (última visita 15 Junio 2005)
[190] El ejemplo que plantea Lessig es el siguiente, a un familiar le prestan o regalan un CD de mp3 sacado de napster que luego copia en su notebook y luego lo lleva a su universidad, y esa universidad por diferentes motivos colabora con la RIAA, es posible que el familiar sea identificado como criminal, ahora bien si esa universidad puede tener políticas que impliquen que el buen uso que se le da a Internet incluye no violar las leyes de propiedad intelectual y las sanciones a dicha conducta pueden ser diversas. A modo de ejemplo puede incluir el prohibir el uso de la red informática al alumno o incluso la expulsión de este.

universidades, colegios etc. La intimidación funciona de la siguiente manera RIAA inicia demandas por montos astronómicos por concepto de daños. El usuario tiene derecho a defenderse, y se considera inocente pero el costo de defenderse es tan alto que termina transando con los demandantes. El análisis que realiza el usuario es el siguiente: si gano el juicio solo me queda un trozo de papel que dice que soy inocente, pero quedo endeudado, ahora bien siempre está la posibilidad que pierda, y en ese caso si que terminaría en muy endeudado. Así, cuesta más defenderse que llegar a un acuerdo[191].

El ejemplo que utiliza Lessig, y que pone de manifiesto lo absurdo que puede llegar a ser el sistema, es que un estudiante de una Universidad dedicada a las tecnologías de la información crea un buscador. La red de computadores de la universidad esta diseñada para acceder a Internet, pero a la vez es una red interna. Lo que "crea" este estudiante es un buscador de intranet, nada muy novedoso, pero sí útil. El índice generado por el buscador incluía imágenes, que los estudiantes habían puesto en sus propias páginas; copias de apuntes o de notas de investigación; copias de folletos informativos; cortos de cine creados por los estudiantes; folletos de la universidad--básicamente cualquier cosa que los usuarios ponían a disposición de la comunidad al ponerlos en una carpeta pública en su ordenador. También incluía archivos musicales que correspondían a ¼ del total de archivos en el buscador.

Por concepto de esos archivos y por ser el operador, la demanda asciende a 15 millones de dólares, además de la estigmatización al ser considerado delincuente. Lo

[191] Lessig con desprecio llama a este proceso de intimidación como mafia organizada e inmoral, por cuanto la industria de la música siempre ha señalado que las infracciones a la propiedad intelectual en el ciberespacio es tanto una cuestión legal como una cuestión moral, y se pregunta donde esta la moral en demandar por sumas astronómicas y quedarse con el dinero de los estudiantes, o forzar a estos a que no puedan utilizar las redes informáticas o no pueden trabajar en algunos sectores de la informática. *"Un mundo que amenaza con 150.000 dólares por una sola violación voluntaria de copyright, y que exige decenas de miles de dólares para siquiera defenderte contra una demanda por violación de copyright, y que jamás le devolverá a alguien acusado injustamente nada de los costes que sufrió por defender su derecho a hablar--en ese mundo, las regulaciones pasmosamente amplias que llevan el nombre de "copyright" silencian la palabra y la creatividad. Y en ese mundo, hace falta una estudiada ceguera para que la gente siga creyendo que vive en una cultura que es libre.",* LESSIG, Lawrance, "Cultura Libre", op. cit. 66.

absurdo es que se trata de un alumno experimentando con una tecnología existente hace algún tiempo, en una universidad en la que estaba estudiando informática en que la meta es experimentar con la tecnología. Nada nocivo según lo que nos dictaría el sentido común, pero al parecer el sentido común no es muy común encontrarlo en estos tiempos[192].

Pasemos al Tratado de Libre Comercio con Chile. En él, Chile se compromete a establecer un sistema de notificación y bajada de los contenidos infractores a la propiedad Intelectual. Así, el TLC señala que "*para los efectos de la notificación y el proceso de bajada de las funciones (b) (ii) _ (iii) i (iv), (estos es caching, hosting y linking) cada parte establecerá procedimientos adecuados mediante un proceso abierto y transparente establecido en su legislación interna, para notificaciones efectivas de supuestas infracciones y contra notificaciones efectivas por parte de aquellas personas cuyo material fue retirado o inhabilitado por equivocación o identificación errónea*[193].

Los sistemas denominados de notificación y bajada o retirada tienen antecedentes en el Derecho comparado. Así, se encuentra en la DMCA Norteamericana, donde opera de la siguiente manera: 1-El titular del derecho objeto de infracción debe notificar al servidor la existencia del contenido infractor. 2- Al recibir la notificación (formalmente correcta), el servidor debe retirar o bloquear el acceso al material descrito en la misma.3- El sistema de contra notificación, al retirar o bloquear el material supuestamente infractor el servidor debe notificarlo al operador del material retirado, entonces el suscriptor presenta una contra-notificación que debe cumplir los mismos requisitos formales que la notificación. 4- El servidor debe dar traslado de la contra-

[192]LESSIG, Lawrance, "Cultura libre", Op. cit. p.65.

193 Capitulo 17 referido a Derechos de Propiedad Intelectual, en el artículo 17.11: Observancia de los derechos de propiedad Intelectual, Limitación de la Responsabilidad de los proveedores de servicios de Internet

notificación al titular del derecho supuestamente infraccionado para que presente una demanda judicial en un plazo determinado sino el material será repuesto[194].

En el ámbito Europeo la Directiva sobre comercio Electrónico señala que: *"la retirada de datos o la actuación encaminada a impedir el acceso a los mismos habrá de llevarse a cabo respetando el principio de libertad de expresión y los procedimientos establecidos a tal fin a nivel nacional. La presente Directiva no afecta a la posibilidad de que los Estados miembros establezcan requisitos específicos que deberán cumplirse con prontitud antes de que retiren los datos de que se trate o se impida el acceso a los mismos"*[195].

La ley española sobre la Sociedad de la Información, establece en su artículo 11 un deber de colaboración de los prestadores de servicios: "*Cuando* ***un órgano competente*** *por razón de la materia hubiera ordenado, en ejercicio de las funciones que legalmente tenga atribuidas,* ***que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España,*** *y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, podrá ordenar a dichos prestadores, directamente o mediante solicitud motivada al Ministerio de Ciencia y Tecnología, que suspendan la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio equivalente de intermediación que realizaran".*

Con respecto a los prestadores de servicio de alojamiento se señala: *1. Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:*

194 XALABARDER, Raquel, "Infracciones de Propiedad Intelectual y la Digital Milenium", en "Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet", Editorial Aranzadi, 2002. pp.130-139

195 Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE 12.07.2002)

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos. Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse"[196].

Lo que hay que hacer notar, es la posibilidad que se tiene que en virtud de acuerdos voluntarios, se proceda a retirar material. Además, se determina cuándo se va a entender que un contenido es ilícito y un órgano competente determina la ilicitud del contenido. La normativa Europea se presenta como más adecuada, por cuanto, lo único que justifica el retiro de un contenido su ilicitud. En el caso de la DMCA, la ilicitud del contenido no esta configurada, se permite la retirada ante una supuesta infracción, con lo cual, se deja la puerta abierta para que ante cualquier eventual infracción, se retiren los contenidos.

En Chile no existe una regulación en torno a un sistema de notificación y bajada, lo cual no implica que ésta no opere. En la práctica, muchas veces, tras un reclamo de un usuario, se bajan determinados contenidos. Es por ello que resulta necesario un somero análisis a una situación que se produce con frecuencia. Existen portales donde se establecen cláusulas que deben ser respetadas por los usuarios, bajo la sanción de ser retirados los contenidos . En términos generales los portales visitados son aquellos que prestan alojamiento para que terceros ofrezcan sus productos, en particular nos referimos a Mercadolibre.cl y DeRemate.cl.

[196] Artículo 16 nº 1 letra a, de la ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE 12.07.2002), p.14.

Una característica, común a ambos sitios, es que declaran proteger la propiedad Intelectual. Ambos tienen programas de protección a la propiedad intelectual. En el caso de Mercadolibre.cl, éste elabora un programa de protección de la propiedad intelectual, que tiene el objetivo de impedir que sean listados u ofrecidos, artículos que violen algún derecho de propiedad intelectual, sea derecho de autor, de patentes, de marcas, modelos y/o diseños industriales.

De este modo, Mercadolibre.cl elabora una lista de artículos prohibidos, en donde no permite la publicación de CDs regrabados, discos compactos ilegales o copias de CDs, películas en formato VCD, DIVX o cualquier otro formato no comercial salvo que sean los titulares de los derechos de autor quienes vendan los artículos. Asimismo, se prohíbe la venta de discos compactos que contengan música en formato MP3, cuando la misma no esté expresamente autorizada por el artista o compañía discográfica propietaria de los respectivos derechos. Lo "curioso", de esta forma de prohibición de artículos, y que nos merece más de un comentario, es que existe cierta discriminación tecnológica. Se impide la publicación de artículos atendiendo primeramente al formato tecnológico (vcd, mp3, divx). Además, el señalar que se impide la publicación de formatos no comerciales, genera dudas. ¿Qué se entiende por formato comercial? ¿Existen formatos tecnológicos que son comerciales a priori? Ambas interrogantes ejemplifican que la técnica usada para elaborar una lista de artículos prohibidos no fue de las mejores.

Ante la existencia de un producto que infringiría los derechos de propiedad intelectual, se debe notificar al portal para que proceda a retirarlo. En el portal se presenta un formulario muy detallado, en donde tras la identificación del titular del Derecho, viene una sección en la cual se debe identificar el objeto infractor junto al derecho intelectual que se considera infringido[197].

[197] El formulario de la notificación puede ser visto en http://www.mercadolibre.cl/org-img/MLseguro/MLC/formulariopppi_CL.doc, (última visita 25 Julio 2005).

Por su parte, el portal deremate.cl[198] solo se limita a señalar que esta prohibido publicar con fines de venta las copias no autorizadas, lo que es acorde a las normas generales sobre propiedad intelectual. Un sistema similar a la notificación es que ante la posibilidad de una infracción se debe informar a un "detective de remate"[199], una especie de moderador que determina finalmente si retirar la publicación. Ahora, la elaboración del formulario de notificación es más precisa en el anterior portal.

Recapitulando, podemos observar que los distintos sistemas de bajada de contenidos y de resguardo a la propiedad intelectual, deben conciliar la legitima protección de sus creadores, la libertad de los contenidos de internet y el debido resguardo al derecho al anonimato, que en el caso de muchos sitios se manifiesta en sus políticas de privacidad. Sin embargo, esta conjunción de deberes y derechos no debe llegar a plantear una persecución irracional acerca de los contenidos en la red ni de sus usos, ya que aquello llevaría a mermar la investigación, los innovadores y todo lo que en definitiva dio mantiene vivo a la red.

5. Registros para facturación y datos de tráfico.

Analicemos ahora lo relativo al almacenamiento de datos necesarios para facturación y su vinculación a la protección del derecho al anonimato. Por razones de facturación el usuario de servicios de telecomunicaciones autoriza contractualmente al operador a registrar y conservar aquellos datos (número de llamadas efectuadas en cada período de facturación, número de los abonados con los que se ha puesto en conexión, duración de la llamada, fecha y hora de éstas, entre otros) que resultan indispensables para determinar el precio justo del servicio prestado y para fundar una reclamación en caso de discrepancia o abuso. Este registro deviene en necesario para el buen desarrollo de la relación contractual, en los términos del artículo 1.546 del Código Civil.

[198] http://www.deremate.com
[199] Formulario para notificar a Deremate en http://www.deremate.cl/servicios/detective/detective.asp?Err=-1, (última visita 20 Julio 2006)

Los operadores de redes de telecomunicaciones y quienes prestan el servicio al público actúan sobre datos personales de tres órdenes distintos:

a) Los datos relativos al contenido de la comunicación.

b) Los datos de tráfico generados por las comunicaciones establecidas durante la prestación del servicio.

c) Los datos de los abonados necesarios para la prestación del servicio pero no generados en los procesos de comunicación.

En este acápite trataremos sobre el punto b, esto es, los datos de tráfico generados por las comunicaciones establecidas durante la prestación del servicio. Los servicios de telecomunicaciones, para los efectos de facturar, registran y conservan estos datos. Ahora bien, por cuánto tiempo pueden conservarse estos datos personales sobre tráfico es la pregunta a dilucidar.

La Unión Europea, respecto a la interrogante recién planteada, ha señalando que los datos sobre tráfico pueden tratarse únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago[200]. Esto significa normalmente lo siguiente: los datos sobre tráfico deberían conservarse mientras sea necesario para permitir el pago de las facturas y la resolución de posibles litigios derivados del pago de estas. Ello implica habitualmente un período de almacenamiento máximo de 3 a 6 meses. Esto sucede en la generalidad de los casos, cuando las facturas se han pagado y no se han impugnado ni son objeto de litigio.

En caso de litigio o impugnación, los datos podrán almacenarse durante un período más largo para facilitar el pago de la factura. Incluso, cuando se haya pagado

[200] Artículo 6 apartado segundo de la directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de las Comunidades Europeas.* 31 Julio de 2002.

una factura, se podría justificar un período más largo de almacenamiento en casos excepcionales, cuando haya indicios concretos de que se va a plantear un conflicto. En tales situaciones, el período de almacenamiento dependerá de las circunstancias particulares de cada caso, para permitir la resolución de los litigios en curso. El período máximo de almacenamiento se comienza a contar desde el momento en que los datos sobre tráfico ya no son necesarios para la transmisión de una comunicación[201].

Es importante adoptar medidas para interpretar, de manera armonizada, el período máximo durante el cual se autoriza a los prestadores de servicios de telecomunicaciones a tratar los datos sobre tráfico a efectos de facturación y de pago de la conexión. Los principios de proporcionalidad y necesariedad son fundamentales al momento de interpretar de manera razonable de las normativas sobre protección de datos [202].

Un proveedor de acceso a Internet tiene un contrato con un abonado a Internet. En este caso, normalmente el proveedor mantendrá un fichero histórico con la dirección IP asignada, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección. Es más, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación.

---

[201] Así lo plantea la directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas

[202] De la aplicación de los principios de proporcionalidad y necesariedad se deriva que el plazo máximo de almacenamiento de 3 a 6 meses para la facturación, a excepción de casos particulares de litigios, en los que los datos podrán tratarse durante un periodo más largo. Además, solamente podrán tratarse los datos que sean adecuados, pertinentes y no excesivos a efectos de la facturación y de los pagos de interconexión. Los demás datos sobre tráfico deberán suprimirse. Dictamen 1/2003 sobre el almacenamiento de los datos sobre tráfico a efectos de facturación. Adoptado el 29 de enero de 2003. Grupo del artículo 29 sobre protección de datos. https://www.agpd.es/upload/B.2.64%29%20wp69-20Dictamen%201.2003.%20Almacenamiento%20datos%20trafico%20facturaci%F3n.pdf, (última visita 15 Junio 2005).

Así pese a lo legítimo y necesario que llega a ser el almacenamiento de datos para efectos de facturación, el real conflicto relacionado con el derecho al anonimato reside principalmente en la escasez de información de que disponen tanto los titulares como los responsables del tratamiento de los datos sobre las disposiciones jurídicas que han de observar. Por ello, en este tema podemos afirmar que el necesario conocimiento de la normativa ha de llevar sin duda a una mejor y mayor protección del derecho al anonimato de los usuarios sin menoscabar la recopilación de datos necesaria para los servicios, materia íntimamente relacionada al tratamiento de los mismos y que analizaremos a continuación.

-Tratamiento de los datos.

En el caso del uso de datos necesarios para la entrega del servicio, esto es los registros de facturación, a primera vista podría parecer que el usuario debido al consentimiento que realiza con el prestador de servicio, no tiene una expectativa razonable de privacidad. Sin embargo, debemos desechar dicha perspectiva.

El análisis que se debe hacer es aquél que permita conciliar el uso de estos datos para facturación con el derecho a la privacidad.

La Directiva 2002/58 sobre la Privacidad y las comunicaciones electrónicas señala en su artículo 7: *1. Los abonados tendrán derecho a recibir facturas no desglosadas. 2. Los Estados miembros aplicarán las disposiciones nacionales a fin de conciliar los derechos de los abonados que reciban facturas desglosadas con el derecho a la intimidad de los usuarios que efectúen las llamadas y de los abonados que las reciban, por ejemplo, garantizando que dichos usuarios abonados dispongan de suficientes modalidades alternativas de comunicación o de pago que potencien la intimidad.* Los datos almacenados relativos al tráfico deben limitarse a los datos

"necesarios". Sólo podrán tratarse los datos que sean adecuados, pertinentes y no excesivos a efectos de la facturación.

Así, podemos ver que en el caso de la necesariedad de registros para facturación no implica una pérdida de la expectativa razonable de privacidad.

6. Cláusulas contractuales.

En este acápite analizaremos algunas hipótesis de expectativa razonable de perdida de privacidad en atención a las actividades y situaciones realizadas por las personas y cómo ello debe conciliarse con el limite que impone el derecho al anonimato. Para ello tomaremos los casos del contrato de trabajo y de prestación de servicios.

6.1 Contrato de Trabajo.

Una de las hipótesis contractuales, en las cuales se puede considerar la protección del derecho a la intimidad en las personas, es el caso de las relaciones laborales y la manera en la cual la intimidad se puede ver afectada, cuándo se establecen cláusulas especiales en el contrato de trabajo. De este modo, cabe cuestionarse si por estas disposiciones se puede limitar la protección a las garantías acerca de la intimidad y, en el caso de las comunicaciones electrónicas, del anonimato. Para el análisis particular comenzaremos por la discusión acerca de la regulación especial de la cual goza el área del derecho laboral, luego acerca de cómo puede plantearse esta regulación en la práctica, para finalizar esbozando algunas líneas sobre la manera en que estos derechos pueden verse aplicados al entorno digital en las relaciones laborales.

La primera distinción que se plantea es por qué las relaciones laborales deben gozar de un estatuto distinto de ponderación de los derechos respecto al derecho civil. En efecto, si las relaciones laborales se insertaran dentro del simple ámbito del derecho

privado, la ponderación sobre la protección al derecho a la intimidad seguiría las reglas generales aplicadas a las cláusulas contractuales. Sin embargo, sabemos que la libertad contractual, tan propia del derecho civil, está limitada dentro del derecho laboral. Lo propio sucede con las restricciones a la intimidad.

Al respecto José Luis Ugarte nos señala: *"La respuesta apunta a destacar el hecho de que la relación laboral posee un elemento absolutamente particular respecto del resto de las relaciones de derecho privado: la existencia de la subordinación o dependencia por parte del trabajador en relación con su empleador, esto es, el ejercicio por parte de un particular de un poder que, admitido por el propio sistema jurídico, recae sobre otro particular. De este modo, los derechos fundamentales, incluida la intimidad, admitidos de pleno en las relaciones laborales, plantea una situación jurídica de complejidad, atendida la existencia de la mencionada subordinación jurídica, que se manifiesta en los poderes que el empleador ejerce sobre el trabajador y que sugestivamente son denominados "potestad jurídica de mando" o "poder de dirección", y cuyo correlato jurídico, con un no menos sugerente nombre, corresponde al "deber de obediencia" del trabajador"*[203].

Por lo tanto, el principal elemento diferenciador de la relación jurídico laboral es la desigualdad de las partes. De este modo una de ellas goza de un poder sobre la otra que hace que el derecho deba preocuparse por proteger especialmente este vínculo. Así es como, si bien en el derecho civil podemos voluntariamente limitar el ejercicio de nuestros derechos, como la intimidad, al vernos enfrentados a una situación de subordinación esta voluntad se pone en pie de fragilidad. En otras palabras, el consensualismo de las partes puede ser vulnerado debido a la supremacía en la posición dominante del empleador.

[203] UGARTE, José Luis. "El derecho a la intimidad y la relación laboral". Dirección del Trabajo, Boletín Oficial Computacional. Publitec S.A. Agosto, 2000. p. 10.

Ahora bien, si existe una diferencia a la limitación contractual al ejercicio de los derechos respecto del derecho civil, la cuestión se traslada en saber en qué consiste esa diferencia. En un primer momento la respuesta parece ser simple: las limitaciones al ejercicio del derecho a la intimidad de parte del trabajador deben resguardarlo de los abusos que pueda cometer el empleador dada su posición. Sin embargo, el problema se complica cuando pensamos en que el empleador trata de justificar la cesión de la intimidad absoluta del trabajador en razón de sus intereses tales como la propiedad o el simple ejercicio correcto de la función laboral. De este modo el asunto se complica.

Así, pareciese ser que los derechos fundamentales gozan de matices que pueden jugar en contra de su ejercicio pleno en este tipo de relaciones. *"La consecuencia de esta vigencia relativa o "matizada" de los derechos fundamentales en las relaciones entre particulares, específicamente en la relación laboral, importa la admisión de restricciones o limitaciones adicionales a dichos derechos, que en otros contextos, fuera de dicha relación, serían inadmisibles jurídicamente(...)"*[204]. Por ello, el problema se traslada a saber cuáles son dichos matices y en qué medida pueden afectar los derechos fundamentales de manera de encontrar un equilibrio con las particularidades propias de la relación laboral.

Nos señala José Luis Ugarte: *"El alcance de la vigencia de los derechos fundamentales en este caso, deberá determinarse mediante un equilibrio de los derechos fundamentales de las partes de la relación jurídica de que se trate..."*[205]. Es por ello, que no podemos determinar de antemano los límites que serán aplicables a las relaciones laborales en resguardo de la intimidad. Corresponden a situaciones particulares que deben ser conocidas caso a caso. Por lo mismo, resulta difícil sino imposible, establecer límites claros y precisos desde la generación de la norma. Por el contrario se deben establecer principios bajo los cuales se establezcan mínimos parámetros sobre los que la

[204] *Ibíd.* p. 12.
[205] *Ibíd.*

relación contractual-laboral pueda desarrollarse sin perjudicar en exceso los derechos del trabajador como del empleador.

Ahora bien, el problema sigue su curso al establecer cuáles son aquellos principios o zonas problemáticas: *"La pregunta nos lleva de lleno al tema de las conductas presumiblemente violatorias de la intimidad del trabajador. Ahora, la falta en nuestro país de decisiones relevantes de los tribunales y de desarrollo doctrinal en esta materia, hace que la respuesta de la pregunta señalada sea bastante tentativa"*[206]. Sin embargo, ello no impide establecer algunas ideas al respecto. Ugarte hace la distinción entre distintas hipótesis primero la invasión de la intimidad físico- espacial y la intimidad moral o afectiva. En la primera comprende controles de la persona, bolsa, efectos, controles médicos y actuación laboral. La segunda comprende indagaciones sobre datos del trabajador y controles extralaborales. Como se aprecia, ninguna de estas hipótesis es clara respecto a las violaciones de intimidad en el ámbito digital, pero a través de algunas de ellas podemos plantear algunos principios al respecto.

En particular, nos referimos al caso del control de los efectos y bolsos. Ello porque en primera instancia podemos de alguna manera asimilar el contenido privado del interior de estos objetos al contenido guardador en un computador. Pero de inmediato nos surge un primer inconveniente: en el caso de los bolsos y efectos normalmente estamos en presencia de objetos que son de propiedad del trabajador o que han sido dispuestos especialmente para resguardar efectos privados. En cambio, no sucede lo mismo con los computadores donde la mayoría de las veces éste se constituye como una herramienta de trabajo para el sujeto. Por ello, es que para lograr algún tipo de analogías es necesario vincularlo a la actuación laboral. Esto es, el control y vigilancia que el empleador hace en vista de verificar el cumplimiento de las labores para las cuales fue contratado.

[206] *Ibíd.* p. 14.

Este tipo de control dice relación únicamente con el necesario para determinar si el trabajador está cumpliendo efectivamente su relación laboral. Sin embargo, nuevamente no hay límites claros. De este modo, se cuestiona si para el empleador es lícito vigilar a los trabajadores en la esfera de sus comunicaciones electrónicas so pretexto de enterarse del correcto o incorrecto uso del computador en su cometido laboral. Nuevamente la jurisprudencia y delimitaciones claras al respecto son esquivas. Ugarte, sin embargo, pone como ejemplo un dictamen de la Dirección del Trabajo relacionado a este tipo de control, en referencia a la medición del tiempo de uso de los servicios higiénicos a los trabajadores.

En efecto, el Dictamen número 4.541/319 del 22 de septiembre de 1998 señala que *“"al dejar establecido el artículo 19 Nº 4 de la Constitución Política de la República que asegura a todas las personas el respeto y protección de la vida privada y pública y a la honra de –la persona y de su familia, se fija un límite a las facultades de administración del empleador –las que desde luego no deben interferir o perturbar el ámbito personal y privado de sus dependientes– lo que a todas luces ocurre al pretender medir el tiempo de permanencia de los trabajadores en los servicios higiénicos”.*

A raíz de lo anterior, sólo podemos aventurarnos a realizar algún tipo de alcance en lo referente a las comunicaciones electrónicas. Si la Dirección del Trabajo se muestra favorable a proteger la intimidad de los trabajadores en áreas sensibles, es posible pensar que en materia de comunicaciones también debemos seguir la misma corriente. Sin embargo, antes de plantear una conclusión, detengámonos un momento más en una interesante opinión del abogado Arturo Prado, en una editorial de la Revista del Colegio de Abogados de Chile:

“De no mediar autorización expresa que permita su divulgación o una resolución judicial fundada y específica justificada en el interés público superior, las comunicaciones -tanto el medio que se utiliza (telefónico, epistolar o telegráfico, o el

propio espacio cibernético) como el mensaje contenido- seguirán siendo impenetrables y prevalecerá la garantía constitucional que ampara la inviolabilidad de toda forma de "comunicación privada", norma que, como quedó claro en la Comisión de Estudios de la Nueva Constitución (Sesión 129°, 12 de Junio de 1975), debe interpretarse con carácter extensivo y sentido común, cualquiera sea el medio técnico o el soporte físico que se utilice para materializar la comunicación hoy o en el futuro.

La circunstancia que en la actualidad se utilice el intercambio de correos electrónicos, como medio habitual para ***facilitar nuestras funciones****, no escapa a esta consideración, no sólo por cuanto en ellos se pone en evidencia el sello personal con que nos desenvolvemos sino porque a través de estas formas de comunicación virtual circula un bien jurídico trascendente y especialmente protegido como es el secreto profesional, núcleo esencial de la relación con nuestros clientes quienes nos abren sus espacios de intimidad con todas sus debilidades, riesgos, preocupaciones y errores"*[207].

De este modo, la intimidad parece sobreponerse aún a las circunstancias laborales. Es decir, el derecho garantizado por la Constitución Política que protege nuestra vida privada debe ser respetado aún cuando frente a él tengamos otro derecho de una contraparte, como el es caso del empleador. Éste podrá ejercer su legítimo derecho de control solamente cuando no lesione derechos elementales de sus trabajadores que merecen de protección más allá de la relación de subordinación en cuestión.

Por lo mismo, tampoco podemos pensar en consideraciones contractuales mediante las cuales el trabajador ceda su protección a la intimidad. Primero, porque dadas las circunstancias de la relación laboral, es de entender que no se contrata en pie de igualdad. Permitir la renunciabilidad de un derecho como la intimidad mediante

[207] PRADO PUGA, Arturo, "Apretando el cerco". Editorial del Colegio de Abogados sobre Incautación de correo electrónico, Revista del Colegio de Abogados N° 32 Noviembre 2004, Santiago, Chile, http://www.abogados.cl/revista/32/editorial.html , (última visita 3 de Junio 2005).

cláusulas contractuales implicaría en la práctica desproteger a los trabajadores de un derecho fundamental en razón de sus necesidades. Segundo, porque como lo menciona el profesor Prado, se trata de un derecho de primer orden, pilar básico en la protección de las garantías constitucionales y, por ello, merecedor de una atención privilegiada por sobre otros derechos.

Así, podemos concluir que en el caso del derecho laboral, las hipótesis planteadas respecto a la protección de la intimidad, reflejado en el anonimato en la red, deben contextualizarse en una relación de desigualdad de los sujetos. En base a ello, tomar en cuenta que la autonomía privada se ve restringida en pos de la protección del trabajador. Si bien, no hay limites concretos para conocer cuándo y en qué momentos se deben proteger los derechos de manera especial, cabe afirmar que sí podemos esperar una protección especial del derecho a la intimidad por los motivos antes dados. Por lo tanto, la futura jurisprudencia laboral debería tender a proteger los derechos al anonimato del trabajador frente a los intentos del empleador de conocer el contenido de sus comunicaciones electrónicas.

6.2 Contratos de Prestación de Servicios.

En el caso de los contratos de prestación de servicios que efectúan los ISP con los usuarios, son por lo general contratos de adhesión. Este tipo de contrato está definido en la llamada Ley de Protección al Consumidor, Ley Nº 19.496 que señala en el artículo 1º número 6 que "*el contrato de adhesión es aquel cuyas cláusulas han sido propuestas unilateralmente por el proveedor sin que el consumidor, para celebrarlo, pueda alterar su contenido".*

Para proteger a la parte más débil de la relación jurídica el legislador regula en forma específica las cláusulas abusivas o leoninas. Sobre este aspecto es que el artículo 16 señala una serie de casos en que las disposiciones no producirán efecto alguno.

Cabe preguntarse si en caso de existir cláusulas que vulneraran el derecho al anonimato, estas podrían ser ineficaces. Para esto habría que comparar la cláusula en cuestión con el catalogo que establece la norma citada.

La última modificación a la Ley de Protección al Consumidor agregó la letra g) al artículo 16 que permite que la lista cerrada y rígida de estipulaciones que se consideran abusivas se amplíe y flexibilice. Es bajo esta letra que se configuraría que estamos en presencia de una cláusula abusiva, dicho artículo 16 en relación con la letra g) nos señala que "No producirán efecto alguno en los contratos de adhesión las cláusulas o estipulaciones que: g) *En contra de las exigencias de la buena fe, atendiendo para estos efectos a parámetros objetivos, causen en perjuicio del consumidor, un desequilibrio importante en los derechos y obligaciones que para las partes se deriven del contrato. Para ello se atenderá a la finalidad del contrato y a las disposiciones especiales o generales que lo rigen. Se presumirá que dichas cláusulas se encuentran ajustadas a exigencias de la buena fe, si los contratos a que pertenecen han sido revisados y autorizados por un órgano administrativo en ejecución de sus facultades legales."*

De esta manera, en caso de encontrarnos ante una cláusula que nos parezca abusiva en relación al Anonimato y Privacidad de los usuarios nos queda recurrir a la letra g) del artículo 16 para intentar declararla ineficaz.

El articulado nos merece reparos en cuanto a técnica legislativa por cuanto hubiera sido preferible establecer un catálogo abierto de cláusulas abusivas. Pese a esto, la letra g) es una puerta que se abre en relación a los contratos de adhesión ya que sin la última modificación dichas cláusulas no podrían ser consideradas abusivas[208].

[208] La última modificación es de fecha 14-07-2004, y con anterioridad a esa fecha el articulado solo incluía desde la letra a) a la f) tras la modificación el artículo 16 quedó de la siguiente manera: Artículo 16.- No producirán efecto alguno en los contratos de adhesión las cláusulas o estipulaciones que:

En estos contratos de adhesión existen cláusulas relativas a la identidad e información de los clientes que son proporcionadas por los propios clientes. Mediante la aceptación, el cliente expresa el consentimiento expreso para que los datos personales sean incorporados a un fichero de datos personales que son objeto de tratamiento automatizado. La finalidad de este tratamiento automatizado de datos personales puede ser muy diversa. Entre ellas se cuentan la adecuación de los servicios a las preferencias y gustos de los clientes, envío de actualizaciones de los servicios, y en general todo lo que implique la gestión, administración, y prestación del servicio.

---

a) Otorguen a una de las partes la facultad de dejar sin efecto o modificar a su solo arbitrio el contrato o de suspender unilateralmente su ejecución, salvo cuando ella se conceda al comprador en las modalidades de venta por correo, a domicilio, por muestrario, usando medios audiovisuales, u otras análogas, y sin perjuicio de las excepciones que las leyes contemplen;

b) Establezcan incrementos de precio por servicios, accesorios, financiamiento o recargos, salvo que dichos incrementos correspondan a prestaciones adicionales que sean susceptibles de ser aceptadas o rechazadas en cada caso y estén consignadas por separado en forma específica;

c) Pongan de cargo del consumidor los efectos de deficiencias, omisiones o errores administrativos, cuando ellos no le sean imputables;

d) Inviertan la carga de la prueba en perjuicio del consumidor;

e) Contengan limitaciones absolutas de responsabilidad frente al consumidor que puedan privar a éste de su derecho a resarcimiento frente a deficiencias que afecten la utilidad o finalidad esencial del producto o servicio;

f) Incluyan espacios en blanco, que no hayan sido llenados o inutilizados antes de que se suscriba el contrato, y

g) En contra de las exigencias de la buena fe, atendiendo para estos efectos a parámetros objetivos, causen en perjuicio del consumidor, un desequilibrio importante en los derechos y obligaciones que para las partes se deriven del contrato. Para ello se atenderá a la finalidad del contrato y a las disposiciones especiales o generales que lo rigen. Se presumirá que dichas cláusulas se encuentran ajustadas a exigencias de la buena fe, si los contratos a que pertenecen han sido revisados y autorizados por un órgano administrativo en ejecución de sus facultades legales.".

En todo contrato de adhesión en que se designe un árbitro, será obligatorio incluir una cláusula que informe al consumidor de su derecho a recusarlo, conforme a lo establecido en el inciso anterior. Lo que se entiende sin perjuicio del derecho que tiene el consumidor de recurrir siempre ante el tribunal competente.

Junto a las cláusulas sobre el tratamiento automatizado de los datos es común que se establezcan las medidas de seguridad que tendrá el encargado del fichero. Lo cual implica adoptar las medidas oportunas de seguridad en sus sistemas y ficheros, y de la misma manera el tratamiento confidencial de los Datos Personales de conformidad con la legislación. No obstante, en caso que las autoridades públicas competentes requieran información sobre los datos contenidos en los ficheros, se les revelará la información, en conformidad con las disposiciones legales y reglamentarias aplicables.

Los datos personales, que habitualmente son proporcionados a las empresas, corresponden a nombre completo y apellidos, dirección de correo , dirección de correo electrónico y teléfono de contacto, horario de contacto, nacionalidad, cédula de identidad, datos sobre la cuenta bancaria.

Otra de las cláusulas que suelen presentar los contratos de prestación de servicios se refiere al correcto uso que deben dar los clientes al servicio. Así, el compromiso de los clientes es a usar el servicio en conformidad con la ley, la moral y buenas costumbres. En algunas ocasiones se incluye una referencia a que los usuarios deben respetar el orden público.

Dentro de estas hipótesis hay conductas que están específicamente prohibidas y que corresponden a grandes rasgos a:

1-Spamming.
2-Escáneo de puertos de otros usuarios[209].
3- Implementación de servicios propios de servidores correo sin la debida autorización.

[209] El escáneo de puertos es una técnica usada para auditar maquinas en las que necesitamos saber que servicios se están sirviendo y de que modo.

A continuación, nos focalizaremos en el fenómeno del Spam, de reciente data y que ha traído consecuencias insospechadas. Ello ya que como objeto de envío y reenvío de datos no deseados puede vulnerar de manera más común y masiva el derecho al anonimato: "*El correo basura es algo más que una simple molestia. Es también una forma común de propagar virus, gusanos y Troyanos"*[210]. Precisamente dentro de estos "troyanos" se encuentra una de las mayores amenazas al anonimato de los usuarios. Veamos el fenómeno en detalle.

El problema del spam para los proveedores de servicios de Internet es que genera saturación del tráfico.[211] Para los usuarios representa una verdadera molestia, se desperdicia ancho de banda, recursos de los servidores y tiempo de los empleados borrando los e-mail no deseados[212].

---

[210] "*El correo basura es cada vez más un medio para el envío de fraudes electrónicos. El fraude electrónico o phishing es un método en línea que utilizan los estafadores expertos para obtener información personal y financiera de los usuarios del correo electrónico. Los correos electrónicos solicitan a los remitentes suministrar el número de la tarjeta de crédito, fechas de expiración, número del carnet de identidad y otra información importante. Puesto que las solicitudes parecen válidas, algunos remitentes divulgan inconscientemente información personal a los ladrones."* http://www.cybercenter.cl/html_cyber2/novedades/Bol12_03_spam.php, (última visita 15 Julio 2006).

[211] ORTUÑO, Mercedes, "El papel de la agencia Española de Protección de datos en la lucha contra el spam.", Memorias del *X* Congreso Iberoamericano de Derecho e Informática, Lom ediciones 2004 p. 255.

[212] Recomendaciones de buenas prácticas para el envío de mensajes publicitarios por correo electrónico. API. Sobre la lucha contra el Spam ver DECLARACIÓN DE CARTAGENA DE INDIAS con ocasión de la celebración del III ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS 25-28 de mayo de 2004 Deben adoptarse medidas técnicas que permitan controlar y establecer filtros al envío de "spam". Estas medidas resultan necesarias, aunque no suficientes para contrarrestar el crecimiento de estas prácticas. En este sentido deberían adoptarse medidas legislativas que disciplinen específicamente la lucha contra el "spam", garantizando los derechos de los usuarios y regulando, en lo que sea necesario, la actividad que desarrollan los diferentes agentes implicados en esta actividad. La colaboración internacional en esta materia permitirá establecer un marco homogéneo, que resulta imprescindible para combatir el "spam", dado el ámbito transnacional del propio fenómeno. Es preciso, además, propiciar e impulsar iniciativas de autorregulación sectorial que complementen y faciliten la aplicación del marco regulatorio sobre la materia. Por último, es imprescindible que se adopten medidas que potencien la concienciación de los usuarios en relación con los perjuicios que la práctica del "spam" les genera. De esta manera, los agentes que posibilitan la propagación de "spam" verán dificultada su actividad por una mayor formación de los usuarios, lo que contribuirá a prevenir activamente esta problemática que presenta múltiples interdependencias.

Definir con exactitud qué es el spam es complejo, pese a ello, existe cierto consenso en definirlo como todo correo electrónico no deseado, no solicitado, no consentido.

El estímulo para realizar spamming es económico."*Se trata de una actividad económicamente rentable: los medios empleados son de muy bajo costo, la rentabilidad es asegurada, aún descontando el valor de multas o penalidades que dicha conducta pudiera traer acarreadas"*[213].

Los problemas que genera el spam en los ISP son descritos por la Asociación de Proveedores de Internet, y se traducen en:

- Aumento del tráfico de correo y por ende mayor utilización de Ancho de Banda, lo cual afecta a los clientes por medio de un acceso más lento (menor ancho de banda disponible).
- Aumento de la utilización de recursos en plataforma de correos. Por ejemplo, del espacio en disco de los servidores de correo. Es un hecho el que las casillas de los clientes llegan a su cuota máxima, con material que en realidad no les interesa ni han solicitado, impidiendo que reciban más correos, que sí son de su interés.
- Atochamiento en el envío y recepción de correo, lo que, además, genera desconfianza respecto de la confiabilidad en el servicio.
- Aumento de los reclamos por Spam, lo cual impacta en el costo y operación del personal de Call Center, operaciones y/o soporte. Existe una suerte de desconfianza de los clientes respecto del mal uso de sus datos (piensan que el ISP distribuye/vende las bases de datos de usuarios), generando una mala imagen para el ISP.

[213] NOUGRERES, Ana Brian, "El Spam: ¿ Dis Función de De-función de redes?", Memorias del X Congreso Iberoamericano de Derecho e Informática, Lom ediciones 2004 p.276.

- Obliga a pensar en invertir o implementar software de monitoreo y control de Spam. Impone la necesidad de hacer desarrollos adicionales para obtener información histórica del uso de servicios de correo, tratando de determinar fuentes de Spam frecuentes, cantidad de Spam en el periodo, comportamiento anómalo de usuarios, entre otros estudios[214].

La actitud de los ISP de incluir entre las conductas prohibidas el spaming se explica por la función de estos en la sociedad de la información, ya que estos son uno de los actores fundamentales en el buen funcionamiento de la red. *"A los ISP compete la aplicación de previsiones estatutarias, reglamentadoras del spam, prohibiéndolo claramente, indicando estados de alarma a los usuarios, sancionando el incumplimiento contractual con medidas de conminación, que busquen un efecto desincentivador del spam, en tanto los réditos económicos que se logran por su intermedio se verían claramente reducidos por importantes multas. Se considera de interés que los ISPs posean acciones estatutariamente delimitadas, claras, que les permitan luchar judicialmente o administrativamente contra los spammers"*[215].

De esta manera, las cláusulas que se incluyen en los contratos y que imponen la abstención de los usuarios de realizar spaming consisten en ejemplificar conductas prohibidas, títulos meramente indicativos y no taxativos. Pensamos que en este caso las conductas de alguna forma podrían también encontrar su límite en un adecuado marco del derecho al anonimato que llevaria a un deber de abstención de spam para procurar su protección.

Algunas conductas que se encuentran prohibidas son: (i) remitir publicidad de cualquier clase y comunicaciones con fines de venta u otras de naturaleza comercial a

[214] Editorial página web de la Asociación de Proveedores de Internet, API., "Efectos o problemas específicos que el Spam produce en los ISP", http://www.api.cl/editorial/sept/efectos.html, última visita 20 Junio 2005.
[215] NOUGRERES, Ana Brian, "El Spam: ¿Dis- Función de De-función de redes?", Memorias del X Congreso Iberoamericano de Derecho e Informática, Lom ediciones 2004 p. 283.

una pluralidad de personas sin que medie su previa solicitud o consentimiento, (ii) remitir cualesquiera otros mensajes no solicitados ni consentidos previamente a una pluralidad de personas, (iii) enviar cadenas de mensajes electrónicos no solicitados ni previamente consentidos.

Además, es de hacer notar, el hecho de la existencia de cláusulas que determinan la suspensión del acceso a los Servicios. Así, se podrá retirar o suspender, en cualquier momento y sin necesidad de previo aviso, a iniciativa propia o a requerimiento de tercero, la prestación de los Servicios a aquellos Clientes que incumplan lo establecido en las condiciones generales.

7. Políticas de Requerimiento.

Vistas ya algunas de las situaciones en donde los derechos de las personas se pueden ver limitados por terceros, analicemos como se pueden requerir dichos datos que al restringir el propio derecho al anonimato llevan a crear un legítimo motivo para conocerlos. En otras palabras, una vez limitado el derecho, hay una expectativa razonable a saber en qué medida han vulnerado dicha garantía.

7.1. Requerimiento de un particular.

En los meses de Enero del Año 2005 se presenció un debate en algunos foros de Internet[216]. Dicho debate se produce en torno a la empresa Yahoo y las políticas de privacidad de su correo gratuito.

El caso denominado Ellsworth, que es el motor de esta polémica, se refiere al soldado Justin Ellsworth, un infante de la marina estadounidense que estaba en servicio

[216] Algunos foros en "Yahoo denies family access to dead marine's e-mail", CNET News.com, http://news.com.com/Yahoo+denies+family+access+to+dead+marines+e-mail/2100-1038_3-5500057.html, 21 de Diciembre 2004, y Who owns your e-mails? BBCNEWS, http://news.bbc.co.uk/2/hi/uk_news/magazine/4164669.stm, 11 Enero 2005, (última visita 20 Junio 2005).

en la ciudad iraquí de Faluya y mantenía una cuenta de correo electrónico con Yahoo a través de la cual escribía mensajes a sus padres. Este murió a los 20 años en la explosión de una bomba en la carretera por la que transitaba. Según el padre del militar, su hijo conservaba un diario de vida en el que ingresaba material de todo tipo para asegurarse que su generación, y las generaciones futuras, tuvieran la versión de alguien que estuvo en la guerra. El padre, quien temía haber perdido algunos de los mensajes, intentó adivinar la clave de su hijo sin ninguna suerte por semanas, por lo que contactó a Yahoo. Esta, sin embargo, tiene una política muy estricta de privacidad, y no permitió el acceso.

El debate se traduce en los foros y portales de noticia en los términos siguientes: ¿a quién pertenecen los mensajes de correo electrónico que una persona ha escrito en su vida? o ¿Quién es el dueño de sus emails?[217] Creemos que el debate estructurado en esos términos es incorrecto. El debate no es en torno a la propiedad de los correos electrónicos una vez que el titular de la cuenta fallece. El debate debe centrarse en las políticas de privacidad de los proveedores de correo electrónico, en su efectivo cumplimiento, y en las expectativas que tienen los usuarios de los servicios de correo del respeto a su privacidad.

Este caso de discusión reciente y a la fecha aun no resuelto, nos sirve para ilustrar el hecho de la ocurrencia de peticiones y requerimientos de particulares a proveedores de servicios de Internet, en este caso un proveedor de correos electrónicos. Lo cual nos lleva a analizar las políticas de privacidad y de confidencialidad de los proveedores correos electrónicos.

La Normativa de Yahoo, sobre confidencialidad, se refiere al uso que se le da a la información personal que se proporciona a dicho proveedor. Esta información incluye

[217] "¿Quién es el dueño de sus emails?", Bbcmundo.com, Miércoles 12 de enero de 2005 http://news.bbc.co.uk/hi/spanish/misc/newsid_4168000/4168443.stm, última visita 2 de Junio 2005

los datos relacionados con la utilización que se ha hecho en el pasado de productos y servicios de Yahoo!. Este proveedor de servicios define lo que se entiende por información personal señalando que *"es el conjunto de datos de usted que le permiten ser identificado, como por ejemplo su nombre, domicilio, correo-e y número telefónico. Son datos privados, es decir, no están disponibles al público"*[218].

Lo que hace la normativa, en cuestión, es definir los datos privados en virtud de la posibilidad de la identificación del sujeto.

Para entender los requerimientos que hacen los particulares a los Proveedores de Servicio de Internet se deben analizar las políticas de confidencialidad y privacidad que establecen los mismos proveedores. Para esto utilizamos sólo algunos proveedores, en específico a los proveedores de correos electrónicos, como parámetros.

La normativa de Yahoo! señala que se puede conservar y revelar el contenido, si así le es requerido por ley o si en buena fe cree que dicha reserva o revelación es absolutamente necesaria para: (a) cumplir con procesos legales; (b) hace valer las condiciones generales del servicio; (c) responder a quejas de que algún contenido viola los derechos de terceras personas; o (d) proteger los derechos, propiedad, o seguridad personal de Yahoo!, sus usuarios y el público[219].

En términos similares, se expresa la política de confidencialidad de Hotmail señalando que es posible que MSN revele y/o acceda a la información personal de los usuarios si ello fuera requerido por ley o en la creencia de buena fe de que tal acción es necesaria para: (a) cumplir las leyes o responder a las órdenes judiciales dirigidas a Microsoft o al sitio, (b) proteger y defender los derechos o la propiedad de Microsoft, incluido todo el conjunto de sitios Web de MSN o (c) actuar bajo circunstancias de

[218] Normativa de confidencialidad de Yahoo, http://privacy.yahoo.com/privacy/e1 , (última visita 15 Junio 2005)
[219] Ibíd.

emergencia para proteger la seguridad personal de los usuarios de los servicios de MSN o del público[220].

Similar es el planteamiento de Gmail. En su normativa se señala que por regla general, cuando alguien envía un mail desde su cuenta de Gmail, esta incluye su dirección de email y su nombre de usuario en la cabecera del email. Más allá de esto, no se divulga información personal, que lo identifique ante terceros, a menos que sea requerido por la ley o por tener una creencia de buena fe que tal acceso o preservación es razonablemente necesarios para (a) satisfacer cualquier ley aplicable, regulación, proceso judicial o petición gubernamental, (b) hace cumplir las condiciones de uso de Gmail, incluyendo la investigación de violaciones potenciales, (c) detectar, prevenir, o tratar de otra manera fraude, seguridad o ediciones técnicas (incluyendo, sin la limitación, la filtración del Spam), (d) responder a las peticiones de ayuda al usuario, o (e) proteger las derechos, o la seguridad de Google, sus usuarios y público[221].

Lo que es común a estas tres políticas de confidencialidad, que hemos nombrado con la finalidad de analizar los criterios y principios que hay detrás, es que las posibilidades de entregar información del contenido esta supeditada a:

1-Al requerimiento que se haga en virtud de disposición legal.

2- Necesariedad basado en la buena fe.

---

[220] *Declaración de privacidad de MSN, (última actualización: septiembre de 2005)* http://privacy2.msn.com/es-la/fullnotice.aspx*, (última visita 15 Mayo 2007).*

[221] As a standard email protocol, when you send an email from your Gmail account, Gmail includes your email address and user name in the header of the email. Beyond this, we do not disclose your personally identifying information to third parties unless we believe we are required to do so by law or have a good faith belief that such access, preservation or disclosure is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or governmental request, (b) enforce the Gmail Terms of Use, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues (including, without limitation, the filtering of spam), (d) respond to user support requests, or (e) protect the rights, property or safety of Google, its users and the public. http://gmail.google.com/gmail/help/privacy.html, política de fecha 14 de Octubre 2005, última visita 4 de Julio 2006.

De esta manera, la expectativa de privacidad de todo usuario de estos servicios está basada finalmente en criterios de necesariedad y buena fe. En el plano de la necesariedad, las diferencia entre estas normativas citadas, es que para algunos debe ser absolutamente necesario (Yahoo!), para otros, basta con ser necesario para cumplir algunos de los fines señalados y en el caso de Gmail existe el criterio de ser razonablemente necesario.

El criterio de buena fe es normado y no queda al arbitrio del proveedor de servicios. Por ello, en caso de que alguno de los proveedores de correo, ya no en virtud de la ley o de un requerimiento judicial, sino en el caso de un requerimiento directamente de un particular, deberá basarse en alguna de las causales mencionadas.

Volviendo al caso presentado al inicio del capítulo, la normativa de confidencialidad de Yahoo! no contempla ninguna hipótesis que permita revelar el contenido de los correos por fallecer una persona. No permiten la entrega del contenido de los correos electrónicos a los padres del militar fallecido. Nos atrevemos a decir que bajo ninguna de las normativas citadas en los otros proveedores de correo se podría haber puesto a disposición del padre los contenidos del correo electrónico[222]. Ante la negativa de Yahoo! a entregar el contenido del correo, la alternativa utilizada por la familia del soldado, es pedir que el padre herede los bienes del hijo[223]. El considerar que los mensajes contenidos en un correo electrónico son parte de los bienes que se pueden heredar implica desconocer el carácter de la comunicación privada de carácter electrónico.

---

[222] La vocería de Yahoo! declaró que se tiene un compromiso con toda persona que abre una casilla de Mail: que la confidencialidad de su correo será preservada. El mostrador, 23 de Diciembre 2004 http://www.elmostrador.cl/modulos/noticias/constructor/noticia.asp?id_noticia=150608 (última visita Enero 2005)

[223] Según el abogado Brian Dayly la petición de herencia de los bienes del hijo concedería, en su opinión, los derechos sobre los mensajes de correo electrónico en polémica entre Yahoo! y la familia de un marine muerto en Irak. El mostrador, 23 de Diciembre 2004 http://www.elmostrador.cl/modulos/noticias/constructor/noticia.asp?id_noticia=150608 (última visita Enero 2005)

7.2. Requerimiento de la Administración Pública.

En este apartado se realizará un análisis de los distintos tipos de requerimiento que puede hacer la administración pública, partiendo con un análisis de jurisprudencia norteamericana. Ello justificado en que en el tema de las nuevas tecnologías, los problemas a los que se ve envuelto Chile ya se han dado en otras latitudes. Por ello, podemos tenerlo como un referente a los problemas futuros que se den en nuestro país. Finalizaremos el apartado con algunas consideraciones en el caso chileno.

La jurisprudencia norteamericana[224] reconoce que los empleados públicos tienen una expectativa legítima de privacidad en su lugar de empleo. No pierden los derechos que les concede la Cuarta Enmienda, en contra de registros y allanamientos irrazonables, por el sólo hecho de trabajar para el gobierno. Cabe mencionar que establecer qué constituye una expectativa razonable de intimidad es algo que habrá que determinar caso a caso. Un aspecto relevante es precisar qué se considera lugar de empleo. La jurisprudencia la definió como *"aquellas áreas y artículos relacionados con las tareas del empleado que de ordinario están bajo el control del superior"*[225].

Para poder establecer en Estados Unidos si un registro, que se produce en el área de empleo, viola la privacidad es necesario llevar a cabo un análisis de tres pasos. El primer paso consiste en analizar las realidades operacionales del lugar de empleo. Se toma en cuenta si el empleado hace uso exclusivo del lugar donde desempeña sus funciones, la naturaleza de los deberes, y si éste tuvo conocimiento que el lugar estaba sujeto a ser registrado. El segundo paso consiste en evaluar la razonabilidad del registro en contraposición con los intereses gubernamentales que pueden justificar la intrusión.

[224] Análisis de algunos pronunciamientos en CESÁREO COHEN, Anthony. Derecho a la Intimidad y el correo electrónico: innovación o invasión. Revista Jurídica Universidad de Puerto Rico, pp. 829-833, Volumen 72, N° 4, año 2003. Texto completo de U.S con Montoya Hernández 473 U.S. 531, de 1985, en http://caselaw.lp.findlaw.com/cgi-in/getcase.pl?court=us&vol=473&invol=531, (última visita 1 Agosto 2006) y U.S con Monroe en http://www.armfor.uscourts.gov/opinions/2000Term/99-0536.htm, (última visita 1 Agosto 2006).

[225] CESÁREO COHEN, Anthony, op. cit. pp.830-831

Por último, el tercer paso requiere determinar si el registro fue razonable en relación con las circunstancias que podrían justificar la intrusión.[226]

Las circunstancias operacionales pueden determinar que el sujeto no tenga una expectativa razonable de intimidad. Así ocurre en el caso en que a un ingeniero civil que trabajaba en proyectos clasificados, era registrado frecuentemente para determinar si la información cualificada como clasificada estaba debidamente protegida[227]. Pese al conocimiento que tenía sobre los registros, guardó un sobre que contenía evidencia sobre relaciones bisexuales que había sostenido. El sobre contenía una indicación al respecto de que era confidencial. Esta indicación genera una expectativa subjetiva en el funcionario, pero no una expectativa objetiva. Por ello, la conclusión del tribunal es que el hecho de que el ambiente de trabajo esté sujeto a registros constantes unido a la anuencia y conocimiento del empleado sobre tales circunstancias remueven cualquier expectativa razonable de intimidad[228].

También se resolvió que la política de la Agencia Central de Inteligencia de limitar el uso de Internet para propósitos oficiales, al igual que notificar acerca de la posibilidad de que se llevaran a cabo auditorias sobre las redes era suficiente para eliminar cualquier expectativa de intimidad que pudiera tener el empleado con respecto al uso de Internet[229].

---

[226] Sobre el caso específico del monitoreo de mails un análisis sobre dicha jurisprudencia en Liability Issues and the Internet Part 1: Electronic Mail Scott F. Uhler, Philippe R. Weiss and Michele M. McGee http://www.lib.niu.edu/ipo/il960266.html , última visita 2 de Junio 2005. En lo principal se exponen los requisitos para determinar cuando se esta en presencia de una invasión a la privacidad y este empleado tiene una expectativa razonable de privacidad en su mail**.** Si un empleado tiene una expectativa razonable de privacidad en su mail, puede ser posible que el empleado demande por los daños civiles por las invasiones de su privacidad por supervisar su E-mail. Los siguientes son varios factores que una corte evalúa cuando se alega este agravio: (1) si la invasión era intencional; (2) la localización y la naturaleza privada de la actividad o empleo; (3) si la invasión es altamente ofensiva de acuerdo a una persona razonable y (4) si un propósito legítimo existió para la infracción. (traducción propia).

[227] CESÁREO COHEN, Anthony, Op. cit. p.830.

[228] CESÁREO COHEN, Anthony, U.S con Simons, op. cit. p.832

[229] Ibíd. El caso, este se inicia cuando el administrador del sistema computacional se percata que la cuenta de la agencia contenía demasiada información. Ante ello, se procedió a realizar una búsqueda dentro de la cuenta utilizando como guía la palabra sexo. Esto trajo como resultado que se obtuvo un

Lo común en el caso norteamericano es la existencia de normas de conducta que regulan los usos que se deben dar a Internet. Además a los funcionarios se les comunica la posibilidad de realizar auditorias de las redes.

En el caso de Chile estas políticas de conducta no se encuentran normadas, sino hasta diciembre del año 2005, tema que se verá en el próximo capítulo[230]. Con anterioridad a esa fecha, los encargados de dictar las políticas de conducta en el uso de Internet correspondía a cada ministerio, subsecretaria, división que componen la administración del Estado a través de instrucciones. En general estas nunca se dictaron. A modo de ejemplo, tomaremos el caso denominado MOP-GATE, en lo que nos parece atinente, para lo cual es necesario hacer un resumen de los hechos.

En el mes de Octubre del Año 2004 se dicta una resolución judicial a cargo de la jueza encargada Gloria Ana Chevesich, donde se ordena la incautación de todos los correos electrónicos de la Coordinadora General de Concesiones entre los años 1997 y 2003. Los funcionarios del Ministerio Obras Públicas (en adelante MOP) sólo se enteran que sus correos están siendo respaldados y almacenados una vez que se ha ordenado la incautación. Dicho respaldo y almacenamiento no contaba con la autorización de los funcionarios.

---

número considerable de resultados provenían de la computadora que utilizaba el empleado. El administrador del sistema entregó una copia del disco duro de la computadora que utilizaba el empleado a un grupo de investigadores de la Agencia Central de Inteligencia que descubrió la existencia de material de pornografía infantil.

[230] Se trata de los Decretos Supremos N° 77 del ministerio general de la presidencia, que aprueba norma Técnica sobre la eficiencia de las comunicaciones electrónicas entre Órganos de la Administración del Estado y entre éstos y los ciudadanos , N°81 del ministerio Secretaria General de la presidencia, que aprueba una "norma técnica para los órganos de la Administración del Estado sobre interoperabilidad de Documentos Electrónicos y N° 83 que aprueba una "Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos", que serán analizados en un capítulo posterior.

Se puede hacer la distinción entre lo que implica por una parte regular el uso que se le da a un medio como Internet y lo que implica vigilar o monitorear, almacenar y registrar los correos electrónicos, donde en estos últimos existe una expectativa de privacidad razonable.

Los problemas que plantea el caso de la incautación de correos electrónicos desde la Coordinadora General de Concesiones (en adelante CGC) son:

1- Desconocimiento por parte de los funcionarios de la CGC del MOP del respaldo y almacenamiento de sus correos electrónicos.

2- No reglamentación respecto al uso de Internet y del correo electrónico.

3- Carácter de comunicación privada del mail .

Sobre el primer punto, hay que hacer notar el hecho que entre los años 1997 y 2003 había funcionarios que ya no trabajaban en el ministerio, y sus correos electrónicos seguían estando almacenados. Una aproximación estima que si los correos estuvieran impresos, corresponderían a unas 14 millones de hojas[231].

Así lo expresa el recurso de protección, *"no fue sino hasta que tomamos conocimiento de la diligencia en cuestión, que nos enteramos que dichos correos electrónicos eran almacenados en la Unidad de Informática de la CGC, obviamente, sin mediar autorización de ninguno de los recurrentes"*[232]. El MOP incurre en un ilícito contra sus propios funcionarios que consiste es una interceptación de una comunicación privada sin estar facultado para ello. Para graficarlo, sería como que determinara grabar,

[231] ARAVENA , Nieves , "Al descubierto lado oscuro de los Mails" , El Mercurio, NIEVES E. SANTIAGO, Viernes 22 de octubre de 2004, Santiago, http://diario.elmercurio.com/2004/10/22/nacional/claves/noticias/AF9303BE-EA6F-4E92-AF58-398915E1F00A.htm?id={AF9303BE-EA6F-4E92-AF58-398915E1F00A}, última visita 15 Diciembre 2005.

[232] Recurso Protección Nº Ingreso 7001-2004 de 14 de Octubre de 2004.

respaldar y luego almacenar por un tiempo indeterminado todas las comunicaciones telefónicas de sus funcionarios.

Eso es manifestado en el Recurso de Protección cuando señalan que "*es preciso advertir que lo que llamó la atención en un primer momento fue que la resolución judicial materia de la presente acción, ha sido dictada respecto de los correos electrónicos de* ***todos*** *los funcionarios de la Coordinación General de Concesiones, sin individualización de persona alguna, que tenga tal calidad (de funcionario) en la referida repartición pública. También produjo asombro la medida judicial para quienes mayoritariamente no somos sujetos formales de ninguna investigación o que ni siquiera hemos sido citados a declarar como testigos en las causas que la Sra. Ministro actualmente investiga, de modo que carecemos de acciones que nos permitan, en el marco de los procesos que la Magistrado instruye, impugnar o cuestionar la resolución dictada"*[233].

El segundo aspecto se refiere a la inexistencia de regulación en el uso de Internet y de las casillas electrónicas[234]. Al respecto, es pertinente recordar que en el censo del año 2002 una polémica, en torno al uso del correo electrónico, se suscita debido a que de algunas reparticiones públicas[235] se expiden correos electrónicos que llaman a los chilenos a no declararse católicos. Dichos correos electrónicos se enviaron en calidad de cadenas, es de hacer notar que pesquisar con absoluta certeza quién es el iniciador de una cadena es algo complejo. Pese a lo anterior, no se reglamentó su uso. Sólo quedó en

[233] Recurso Protección, Op. cit.
[234] Solo con posterioridad en los meses de Diciembre de 2004 y Enero del 2005 se dictan una serie de Decretos Supremos que regulan esta situación. Se trata de los Decretos supremos N° 77 del ministerio general de la presidencia, que aprueba norma Técnica sobre la eficiencia de las comunicaciones electrónicas entre Órganos de la Administración del Estado y entre éstos y los ciudadanos , N°81 del ministerio Secretaria General de la presidencia, que aprueba una "norma técnica para los órganos de la Administración del Estado sobre interoperabilidad de Documentos Electrónicos y N° 83 que aprueba una "Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos".
[235] Específicamente se trató del Consejo Nacional para el Control de Estupefacientes, CONACE, y del Servicio Nacional de la Mujer, SERNAM.

la conciencia de los funcionarios que les tocó vivir la experiencia lo problemático que puede llegar a ser hacer un clic para responder una cadena. [236]

El mal uso del correo trae aparejada la merma de recursos públicos. Muchas veces se utiliza para recibir y enviar mensajes con archivos adjuntos de humor, que no tienen relación con las obligaciones de los funcionarios públicos. Una mala utilización de Internet y del correo electrónico arriesga enormemente cada computador y pone en peligro la seguridad e integridad de todos los equipos de una repartición pública. Un uso inadecuado aumenta el riesgo de tener virus o algún tipo de programas maligno. Una primera fase, para disminuir este efecto negativo, es concientizar a los funcionarios del peligro del mal uso de Internet. En una segunda etapa consistirá en establecer la responsabilidad y las medidas de seguridad que deben respetar los funcionarios en el uso de Internet.

El tercer punto a tratar es la calidad de comunicación privada del correo electrónico. Se debe señalar que los correos electrónicos son utilizados como una herramienta más de trabajo, pero también son utilizados para comunicaciones personales de carácter privado, tales como envío de cartolas de bancos, comunicación con ejecutivos de cuenta, mensajes con familiares y amigos, en los cuales se manifiesta estados de ánimo, creencias religiosas, políticas e incluso filosóficas[237].

---

[236] Insulza acoge reclamo de Cardenal Errázuriz, La Tercera, Santiago, Chile, 4 Febrero 2002, http://tercera.copesa.cl/diario/2002/04/02/02.03.3a.POL.CARDENAL_PT.html, (última visita 31 Mayo 2005).

[237] El recurso de protección interpuesto por los funcionarios lo manifiesta en los siguientes términos: "La ilegalidad y arbitrariedad de la diligencia decretada radica en que, siendo personas ajenas a la investigación judicial, se pretenda abrir y registrar nuestros correos electrónicos, los que contienen nuestra correspondencia personal y privada y que, con prescindencia del dominio del servidor y de los equipos computacionales, en los hechos , se constituye , esa diligencia, en una intervención natural de nuestra intimidad, entendiéndose por tal " aquella zona espiritual del hombre que considera inespecífica, distinta a cualquier otra , independiente de que lo sea; y, por tanto, exclusivamente suya que tan sólo el puede libremente revelar"

El carácter de comunicación privada[238] no depende de la propiedad de los equipos a través de los cuales se realiza esta. El sólo hecho que la propiedad de los computadores no pertenezca a los funcionarios, no le quita el carácter de comunicación privada al correo electrónico. En este sentido, se ha manifestado la Dirección del Trabajo en un dictamen señalando que: "*La experiencia práctica que emana de los hechos y la costumbre, indican que en el ámbito de las relaciones de trabajo, lo habitual y frecuente es que el empleador no pretenda enterarse del contenido de las llamadas telefónicas de sus dependientes, aún cuando la línea y el aparato pertenezcan al empleado*"[239].

Una interpretación extensiva permite concluir que el correo electrónico se encuentra protegido por la Carta fundamental. La constitución preceptúa en al artículo 19 nº 5 que se asegura a todas las personas: "La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley". La Constitución del año 1925 protegía la inviolabilidad de la correspondencia. La comisión Ortúzar entiende que se debe buscar un término más genérico que incorpore a la comunicación telefónica y telegráfica. La conclusión es que el término más adecuado es el de comunicaciones privadas, "*porque comunicaciones cubre todo acto, no sólo los que existen hoy , sino los que pueden existir mañana.(...) La idea es la comunicación privada: puede ser telefónica, telegráfica, epistolar o por otras formas que todavía no se conocen"*[240]. La comunicación privada es aquella en que el emitente singulariza al destinatario, situación que se cumple en el correo electrónico.

---

[238] Comunicación privada es definida por la Comisión Ortúzar como toda aquella en que el emitente singulariza al destinatario. Actas Oficiales de la Comisión Constituyente, sesión 129, celebrada el día 12 junio de 1975, p.10

[239] Dictamen de la Dirección del Trabajo Nº 260/19, SANTIAGO, 24.01.2002, De acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores

[240] Actas Oficiales de la Comisión Constituyente, sesión 129º, celebrada el día 12 de Junio de 1975. p. 10-12.

Ahora bien, qué entendió la jurisprudencia al respecto. La Corte de Apelaciones de Santiago señala: *"**si el contenido de los correos electrónicos, medio de comunicación de reciente data, se encuentran o no para el constituyente comprendidos dentro la documentación privada que resguarda nuestra Carta Fundamental, o si la circunstancia de que se utilizara por funcionarios para fines particulares dicho medio de comunicación usando equipos computacionales pertenecientes al Fisco de Chile, le pueda restar dicho carácter, en razón que ésta es una cuestión que a juicio de los sentenciadores no corresponde dilucidar en esta instancia.** A mayor abundamiento, y de estimar que en las cintas ordenadas incautar, junto con la información propia del servicio, también se contendrían correos electrónicos de carácter personal y privado de los funcionarios estatales, por la indivisibilidad de la misma, hacía imposible que la señora Jueza estuviera en condiciones de identificar y clasificar, a priori, cada uno de los documentos contenidos en ellas"*[241]. *(*negritas nuestras)

Parece increíble, pero la decisión de la Corte es no manifestarse. Obviar un punto trascendente de la discusión.

Los jueces deberían haber realizado un proceso de traducción. Las diferentes tecnologías son lenguajes diferentes, y la finalidad es hallar una interpretación de la Constitución que preserve su significado independientemente de las tecnologías.

Los jueces son pasivos, no se definen en torno a un tema fundamental, como es que el correo electrónico encuentra protección constitucional. Así lo expresa Lessig, al señalar su temor en torno a los tribunales. Así "*cuando no existe una respuesta acerca*

[241] Sentencia Iltma. Corte Apelaciones de Santiago, de Fecha 6 de Diciembre 2004, que rechaza la acción de protección interpuesta por los funcionarios del Ministerio en contra en contra de la Ministra en visita extraordinaria Sra. Gloria Ana Chevesich, por haber dictado en la causa rol Nº 15.260 XS. Letra D, seguida en el Décimo Séptimo Juzgado del Crimen de Santiago, la resolución de fecha 15 de septiembre de 2004, en la que ordena la incautación de los correos electrónicos de todos los funcionarios de la Coordinación General de Concesiones del Ministerio de Obras Públicas, emitidos entre los años 1997 y 2003, Rol Nº 7.001-2.004

de la manera de proceder en la práctica del Derecho Constitucional disponemos de dos tipos de respuestas. Una de ellas es de carácter pasivo: los tribunales han de limitarse a dejar las decisiones en manos de otros. La segunda respuesta posee un carácter más activo: los tribunales han de hallar un modo para articular los principios constitucionales no presentes en el momento de la redacción. La primera respuesta constituye un modo de no hacer nada, mientras que la segunda plantea una manera de activar un debate acerca de los principios constitucionales como medio para enfrentarse a nuevas preguntas y darles respuestas"[242].

En definitiva, existen dos violaciones, una es el respaldo que hizo el MOP de los correos electrónicos de los funcionarios, sin autorización y luego la incautación de los correos electrónicos por parte de la justicia. En la opinión del Colegio de Abogados "*de no mediar autorización expresa que permita su divulgación o una resolución judicial* ***fundada*** *y* ***específica*** *justificada en el interés público superior, las comunicaciones - tanto el medio que se utiliza (telefónico, epistolar o telegráfico, o el propio espacio cibernético) como el mensaje contenido- seguirán siendo impenetrables y prevalecerá la garantía constitucional que ampara la inviolabilidad de toda forma de comunicación privada, norma que, debe interpretarse con carácter extensivo y sentido común, cualquiera sea el medio técnico o el soporte físico que se utilice para materializar la comunicación hoy o en el futuro*"[243].

La idea anterior manifiesta que los procesos judiciales se dirigen en contra de determinados sujetos por la eventual responsabilidad personal que les pudiese asistir en los hechos delictivos que se investigan, no en contra de toda una institución

[242] LESSIG, Lawrance, "El código y otras leyes...", Op. cit. pp. 225-226.
[243] PRADO PUGA, Arturo, "Apretando el cerco". Editorial del Colegio de Abogados sobre Incautación de correo electrónico, Revista del Colegio de Abogados N° 32 Noviembre 2004, Santiago, Chile, http://www.abogados.cl/revista/32/editorial.html , (última visita 3 de Junio 2005).

Tanto en el caso de los Estados Unidos como en el caso chileno, vemos características comunes que nos hacen plantear que en un mundo globalizado si no se pone acento en la protección de las comunicaciones derivaremos a un sistema en constante vigilancia y además paranoico al tratar a todos los usuarios de las nuevas tecnologías como sujetos peligroso y potenciales delincuentes[244]. Hay que afirmar que el correo electrónico tiene protección constitucional. La práctica de respaldar los correos electrónicos y su posterior almacenamiento, como la incautación de correos electrónicos no tiene justificación[245].

Se debe poner atención en el planteamiento que señala que la protección de la libertad y los derechos fundamentales se ve reducida, a medida que los costos de los procesos de monitorización, respaldo y almacenamiento se vean, a su vez, reducidos. Para ello, un ejemplo; es técnicamente factible grabar y almacenar todas las conversaciones telefónicas de los funcionarios de una repartición pública o de una empresa. Sin embargo, monitorizar y grabar las comunicaciones por teléfono es altamente costoso. En cambio, con las nuevas tecnologías el respaldar y almacenar correos electrónicos se torna en algo que no presenta altos costos. Ésto implica que *"los altos costos del control nos proporcionan un cierto grado de libertad"*[246]. La pregunta que se hace Lessig al respecto es si con la reducción de costos ¿disminuirá también la

---

[244] SANCHEZ BRAVO, Álvaro, "Espionaje en el Ciberespacio" http://www.ieid.org/congreso/ponencias/Sanchez%20Bravo,%20Alvaro%20A.pdf , ponencia del II Congreso Mundial de Derecho Informático, España; Cuna de un Mundo Global, Facultad de Derecho Universidad Complutense de Madrid, 23-27 de Septiembre de 2002, (última visita 3 de Junio 2005). Critica la manifestado por John Ascroft, Secretario de Justicia norteamericano tras la aprobación de la Patriot Act que entre otras habilitaciones permite al gobierno de USA el espionaje en Internet el que señaló que *"Vamos a perseguir el terrorismo en Internet, vamos a abrir sus correos electrónicos ante de que ellos los hagan, a escuchar sus mensajes telefónicos, a interceptar sus conversaciones"*.

[245] Jaramillo, Paula y Álvarez Daniel. **"**PRIVACIDAD DEL CORREO ELECTRÓNICO" http://www.derechosdigitales.org/node/15 , (última visita 31 Mayo 2005). *"El correo electrónico está protegido constitucionalmente, de manera tal que su registro, interceptación o apoderamiento de su contenido, son ilícitos constitucionales y constituye una flagrante violación de los derechos humanos, siendo –en el caso de los funcionarios del MOP- causal para recurrir a los organismos del sistema internacional o interamericano de protección de dichos derechos. Lo anterior resulta de vital importancia si consideramos que la intimidad es una de las principales garantías que protegen al individuo frente a intromisiones ilegítimas del Estado o incluso de otros particulares."*

[246] LESSIG, Lawrance, "El código y otras leyes..." ,op. cit. p. 268.

protección a la privacidad? Al parecer por lo que se puede apreciar por la monitorización de los correos electrónicos en las empresas y por el respaldo de mails producido en el MOP, la protección disminuye, situación que se presenta como preocupante. La privacidad y el anonimato no pueden depender de los costos de control.

7.3. Confidencialidad y Seguridad en las Comunicaciones electrónicas con el Estado.

Entre diciembre del año 2004 y enero del 2005, se dictan una serie de decretos, que hacen referencia a aspectos de importancia para el desarrollo y utilización del documento electrónico, en la Administración del Estado[247]. Estos se resumen en:

1-La regulación de la comunicación electrónica y el almacenamiento del documento electrónico. (Decreto Supremo Nº 77).
2-Interoperabilidad de los documentos electrónicos. (Decreto Supremo 81)
3-La regulación de la seguridad y confidencialidad del documento electrónico. (Decreto Supremo 83).

[247] El 23 de Diciembre del año 2004 fue publicado el Decreto Supremo nº 77, del Ministerio General de la Presidencia, que aprobó la normativa técnica sobre la eficiencia de las comunicaciones electrónicas entre Órganos de la Administración del Estado y entre éstos y los ciudadanos. Esta norma regula de forma general y supletoria las comunicaciones que se realicen por medios electrónicos, que tengan lugar entre los órganos de la administración del Estado y entre éstos y las personas, en todos aquellos ámbitos no regulados por otras normas legales, reglamentarías o administrativas específicas.
En esta misma fecha, fue publicado el Decreto Supremo N° 81, del Ministerio Secretaria General de la Presidencia, que aprobó la normativa técnica para los órganos de la Administración del Estado sobre interoperabilidad de Documentos Electrónicos. Se establece, en dicho cuerpo legal, las características mínimas obligatorias de interoperatividad, que deben cumplir los documentos electrónicos en su generación, envío, recepción, procesamiento y almacenamiento. Lo anterior, tanto en los órganos de la Administración del Estado, como en las relaciones de la ciudadanía y el sector privado con dichos órganos y las demás cuya aplicación se recomienda. Además, establece tres niveles progresivos de implementación estableciendo plazos para ello. Por último, el 12 de Enero del año 2005 se publica el Decreto Supremo nº 83, que aprueba una "Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos", que establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los Órganos de la Administración del Estado.

Análisis Decreto Supremo Nº 77.

El artículo 54 del Decreto Supremo 181[248] dispone la elaboración de la norma técnica que permita que las comunicaciones por medios electrónicos, efectuadas entre los órganos de la Administración del Estado, y de éstos con los ciudadanos operen de manera efectiva y eficiente. El Decreto Supremo N° 77 viene a cumplir esa disposición. Se ha señalado que esta normativa viene a "*instrumentalizar legal y administrativamente -de la mano de una herramienta muy común como es el correo electrónico y la red Internet- el ejercicio del derecho de petición que consagra la Carta Fundamental. Todo enmarcado en lo que es el gobierno Electrónico cuyo desarrollo requerirá una plataforma integrada de servicios"*[249].

El artículo 19 N°14 de la Constitución de 1980 asegura a todas las personas el derecho de presentar peticiones a la autoridad, sobre cualquier asunto de interés público o privado, sin otra limitación que la de proceder en términos respetuosos y convenientes

El decreto no define lo que se entiende por comunicación electrónica. Es posible entender que esto se realizó para no encasillar el concepto. Lo cuestionable del decreto es que reduce arbitrariamente lo que el Estado comprenderá por comunicación electrónica. Así el inciso segundo del artículo 5º dispone que *"sólo se considerarán aquellas comunicaciones electrónicas que contengan preguntas consistentes y fundadas, que digan relación materias propias de la competencia de cada servicio público que, en consecuencia, requieran de un pronunciamiento formal".* La disposición transcrita es inconstitucional, ya que establece mayores requisitos que los que establece la Constitución en su artículo 19 nº 14. El decreto no señala que debe considerarse por pregunta consistente y fundada, ni tampoco al responsable de determinar cuando se

[248] El Decreto Supremo nº 181 de 2002 del Ministerio de Economía, Fomento y Reconstrucción aprobó el reglamento de la Ley 19.799 sobre documento electrónico, firma electrónica y la certificación de dicha firma.

[249] JIJENA, Renato "Gobierno, Comunicaciones Electrónicas y Ciudadanos", fecha publicación 07-01-2005, http://www.tecnogestion.cl/articulo.php?uid=100, (última visita 1 de junio 2005).

requiera un pronunciamiento formal. Es posible que arbitrariamente un servicio público estime que no es necesario responder. La norma descrita es discriminatoria de la tecnología, toda vez que el derecho de petición resulta más sencillo ejercerlo a través de los medios tradicionales, esto es el soporte papel que por el soporte electrónico.

La tecnología debe facilitar el acceso de las personas a los órganos de administración del Estado, y no restringir ese acceso. Un avance, en este sentido, se visualiza al establecer la obligatoriedad de designar una o más direcciones electrónicas aptas para recibir la comunicación de las personas.

En su artículo 6° señala que "*Deberá quedar constancia de la transmisión y recepción de las comunicaciones efectuadas por medios electrónicos e identificarse el remitente, destinatario, fecha y hora de las mismas. Con la finalidad de asegurar la constancia de la transmisión y recepción, los órganos de la Administración del Estado que hagan uso de medios de comunicación electrónicos, deberán conservar los registros de estas comunicaciones por un período de tiempo que no podrá ser inferior a 6 años*."

Respecto al artículo anterior, cabe hacer los siguientes comentarios. Llama la atención el tiempo durante el cual deben permanecer los registros para el almacenamiento. Los ISP tienen deberes de registro que le impone el Código Procesal Penal, en donde el tiempo de duración de los registros es de 6 meses. Cabe preguntarse si a los ISP se le pueden plantear dudas, en cuanto a qué tiempo de mantención de registros están obligados. También cabe cuestionarse el plazo de 6 años como mínimo. ¿Qué justifica ese plazo? ¿Por qué 6 años, pudieron ser más o menos?. Ahora bien, se establece un mínimo pero nunca se establece un máximo. Se puede almacenar por tiempo indefinido. La cantidad de información almacenada puede llegar a tal nivel que ya no sea útil, y se presente su almacenamiento como innecesario.

Análisis Decreto nº 81.

El tema fundamental de este decreto es lograr la interoperabilidad del documento electrónico. Interoperabilidad se define como la capacidad, conocimiento y acuerdo de dos o más partes de un todo para interoperar. A su vez que interoperar es operar o funcionar dos o más partes de un todo de manera conjunta y mancomunada para lograr un fin determinado. Interoperabilidad significa "conversar". Significa intercambiar información y comprender esa información de la misma forma en que el otro lo hace. Para conversar, son necesarias dos cosas: que haya un canal de comunicación, y que exista un lenguaje común. El canal común no es otro que Internet, el lenguaje que se va a utilizar en virtud del decreto nº 81 es XML.

XML**,** abreviatura del inglés e**X**tensible **M**arkup **L**anguage, es una tecnología desarrollado por el World Wide Web Consortium (W3C), una organización sin fines de lucro que reúne a empresas y personas naturales en el mundo, cuya dedicación es desarrollar los estándares que surgen como una exigencia en Internet. XML permite la compatibilidad entre sistemas para compartir la información. Las ventajas de este lenguaje son:

1-Es extensible, lo que implica que una vez diseñado un lenguaje y puesto en producción, es posible extenderlo con nuevas etiquetas, de manera de que los antiguos consumidores de la versión antigua aún puedan entender el nuevo formato.

2-Es sencillo entender su estructura y procesarlo. Mejora la compatibilidad entre aplicaciones.[250]

El fin determinado que justifica la interoperabilidad es lograr la interconexión de todos los servicios públicos, para que los órganos del Estado sean capaces de ofrecer

---

[250] Metadatos y documentos xml/rdf para recuperación, *http://metadatosxmlrdf.50webs.org/xml.html*, (última visita 15 mayo 2007).

servicios e información al ciudadano de manera eficiente y transparente, velando por su participación y acceso. Se establecen niveles y plazos para la implementación de esta norma. El nivel 1 se refiere a lo que el servicio recibe desde el exterior. El nivel 2 a lo que el servicio genera hacia el exterior El nivel 3 se refiere a lo que el servicio hace en su interior. El plazo final para el funcionamiento de la interoperabilidad es Diciembre año 2009. *"El sueño es tener una arquitectura de interoperabilidad el año 2010"*[251].

La interoperabilidad es la base de la ventana única. Se pretende integrar un sistema que entregue una adecuada atención a la ciudadanía en un sólo lugar, lo que es parte del gobierno electrónico. Las prioridades en el gobierno electrónico es preparar a las instituciones y servicios gubernamentales para los cambios que deberán enfrentar y difundir los beneficios ofrecidos por este canal. Para lograr los fines del gobierno electrónico la base técnica es fundamental, el desarrollo del lenguaje común que mencionamos al principio.

Un aspecto relevante del decreto es que regula el expediente electrónico y el sobre electrónico. El expediente electrónico es aquel documento electrónico compuesto por una serie ordenada de actos y documentos representados en formato electrónico, dispuestos en estricto orden de ocurrencia, de ingreso o egreso en aquél, y que corresponde a un procedimiento administrativo o asunto determinado. El sobre electrónico es el contenedor capaz de incorporar uno o más documentos electrónicos, además de una o más firmas asociadas a dichos documentos, cuando se encuentren firmados[252]. Ambos deben respetar la integridad, autenticidad y confidencialidad de los documentos.

La relevancia para nuestra tesis está dada porque ese lenguaje, que es el fundamento de la interoperabilidad, debe respetar el anonimato de los usuarios.

[251] BRAVO LILLO, Cristian, "¿Que es interoperabilidad?", http://www.kind.cl/kind/index2.php?option=com_content&do_pdf=1&id=9 ,19 Septiembre 2006, última visita 18 de Abril 2007).
[252] Artículo 5º letras e) y n) decreto supremo 81.

También resulta importante el tratamiento que haga la administración pública del expediente y del sobre electrónico.

Análisis Decreto nº 83.

Los alcances de esta norma son amplios, ya que abarca desde acciones cotidianas de protección de los equipos computacionales, como es no consumir alimentos ni bebida en las cercanías de un sistema informático, hasta una completa política de seguridad institucional.

La idea que subyace a la norma es exponer un código de buenas prácticas para la de seguridad de la información en los órganos del Estado, que va de lo básico a lo más complejo. Se indica en general los ámbitos que hay que enfrentar, pero no describe cómo se debe implementar. Las decisiones finales sobre como disminuir los riegos corresponden a cada jefatura.

De acuerdo al artículo 6 del Decreto Supremo N° 83 la seguridad del documento electrónico se logra garantizando los siguientes atributos esenciales:

a) Confidencialidad;

b) Integridad;

c) Factibilidad de autenticación, y

d) Disponibilidad.

Para lograr esa seguridad se establecen una serie de acciones en el artículo 7°[253]. En virtud que desarrollar todas esas acciones puede resultar innecesario es que,

[253] Artículo 7º.- Los atributos esenciales que aportan seguridad al documento electrónico se obtienen y sostienen mediante la ejecución permanente de las siguientes acciones:
a) Desarrollar y documentar políticas de seguridad de uso, almacenamiento, acceso y distribución del documento electrónico y de los sistemas informáticos utilizados en su procesamiento;
b) Diseñar y documentar los procesos y procedimientos para poner en práctica las políticas de seguridad;
c) Implementar los procesos y procedimientos señalados precedentemente;
d) Monitorear el cumplimiento de los procedimientos establecidos y revisarlos de manera de evitar incidentes de seguridad;

dependiendo de la función de cada organismo de la administración del Estado, el artículo 8° en su inciso 2° señala que para la consecución y mantención de tales atributos por parte de cada órgano de la Administración del Estado estarán sujetas a la consideración de factores de riesgo y factores de costo/beneficio. Estos últimos podrán invocarse mediante una resolución fundada del jefe de servicio correspondiente, basada en un estudio de análisis de riesgo y/o costo/beneficio.

Si recordamos lo sucedido en el caso de la incautación de correos electrónicos del Ministerio de Obras Públicas apreciamos que no existían normativas para el uso del correo electrónico por parte de los funcionarios públicos, como tampoco el uso que se debe dar a Internet. El Decreto Supremo 83 ordena a los jefes de servicios que dicten instrucciones que regulen esas materias. El artículo 20 lo señala:

> El Jefe de Servicio deberá impartir instrucciones para la seguridad de los documentos electrónicos y los sistemas informáticos, respecto de las siguientes materias:
>
> a) Uso de sistemas informáticos, con énfasis en prohibición de instalación de software no autorizado, documentos y archivos guardados en el computador.
>
> b) Uso de la red interna, uso de Internet, uso del correo electrónico, acceso a servicios públicos, recursos compartidos, servicios de mensajería y comunicación remota, y otros.
>
> c) Generación, transmisión, recepción, procesamiento y almacenamiento de documentos electrónicos.
>
> d) Procedimientos para reportar incidentes de seguridad.

Un especial énfasis pone esta normativa a la regulación del correo electrónico. Las instrucciones que se dicten sobre el uso seguro del correo electrónico deben

---

e) Concientizar, capacitar y educar a los usuarios para operar los sistemas informáticos de acuerdo a las exigencias establecidas;
f) Definir y documentar los roles y responsabilidad de las entidades e individuos involucrados en cada una de las letras anteriores.

contener al menos una serie de puntos que van desde explicar la vulnerabilidad del correo electrónico hasta la peligrosidad de virus al abrir archivos adjuntos[254].

Un tema importante es el del almacenamiento y respaldo de los documentos electrónicos. El artículo 24 señala que deberán realizarse copias de respaldo de la información y las aplicaciones críticas para la misión de la institución en forma periódica, en conformidad con las siguientes reglas:

a) La periodicidad con que se realizarán los respaldos de los computadores personales de la institución que estén asignados a usuarios, deberá explicitarse y no podrá ser menor a 1 respaldo anual;

b) La periodicidad con que se realizarán los respaldos de los sistemas informáticos y los equipos no contemplados en el punto anterior, utilizados en el procesamiento o almacenamiento de documentos electrónicos, deberá explicitarse y no podrá ser menor a un respaldo mensual;

c) Deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo. Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 2 años, para

[254] El artículo 25 señala que las instrucciones deben incluir al menos:
a) Una advertencia sobre la vulnerabilidad del correo electrónico a modificaciones o accesos no autorizados;
b) Una advertencia sobre los peligros asociados a la apertura de archivos adjuntos y/o a la ejecución de programas que se reciban vía correo electrónico;
c) La responsabilidad de no divulgar contraseñas de acceso al correo electrónico;
d) Una advertencia sobre la inconveniencia de almacenar contraseñas de acceso al correo electrónico en el mismo computador desde el cual se accede el correo electrónico;
e) Indicaciones sobre la elección de contraseñas seguras de acceso al correo electrónico;
f) Una recomendación sobre la conveniencia de que los usuarios tengan cuentas de correo electrónico distintas para efectos de su uso personal;
g) Un instructivo de cuándo no usar el correo electrónico;
h) Una prevención sobre la necesidad de comprobar el origen, despacho, entrega y aceptación mediante firma electrónica, e
i) Una precisión de las responsabilidades que corresponden a los usuarios en caso de comprometer a la institución, por ejemplo, con el envío de correos electrónicos difamatorios, uso para hostigamiento o acoso, compras no autorizadas, etc.

asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales;

d) Deberá almacenarse en una ubicación remota, un nivel mínimo de información de respaldo, junto con registros exactos y completos de las copias de respaldo y los procedimientos documentados de restablecimiento. Esta instalación deberá estar emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. En ámbitos críticos para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo;

e) Los respaldos deberán cumplir con un nivel apropiado de protección física de los medios, consistentes con las prácticas aplicadas en el sitio principal. Los controles asociados a los dispositivos del sitio de producción deberán extenderse para abarcar el sitio de respaldo.

f) Deberán consignarse plazos de retención de los respaldos de la institución, así como cualquier necesidad de realización de respaldos que estén permanentemente guardados, y

g) Deberán utilizarse medios y condiciones físicas de almacenamiento que garanticen una vida útil concordante con los plazos definidos en el punto precedente.

Un hecho al que hay que hacer hincapié, respecto al decreto N° 83, es que en un análisis general de sus artículos, se puede presenciar el énfasis que se pone en que las instrucciones que se dan sobre el uso de Internet, correo electrónico, políticas de seguridad, etc, queden documentadas y con ello que sean de conocimiento de los usuarios[255].

[255] A modo de ejemplo el artículo 7° del Decreto Supremo N° 83.

Esta normativa viene a dar respuesta a una serie de cuestionamientos que se hicieron a la Administración Pública[256]. Entre estos que los funcionarios no tuvieran un instructivo de cuándo no usar el correo electrónico[257].

La conclusión de este apartado es que el tema de la técnica es fundamental, y debe ser entendida en profundidad, pero no debe enceguecer. La interoperabilidad es necesaria, pero no al costo del derecho de las personas. La inconstitucionalidad del decreto nº 77 es un ejemplo.

[256] Recordar el caso MOP Gate y la incautación de correos electrónicos.
[257] Es factible que algún grado de relevancia en la elaboración de esta normativa hayan tenido los sucesos de Octubre del 2004.

Capitulo IV.

Conclusiones.

A lo largo de este trabajo, nos planteamos el problema que existe entre el derecho a la intimidad y privacidad, el derecho al anonimato y las comunicaciones en la red. Para ello analizamos los diversos conceptos y su importancia en el mundo jurídico, para así poder encontrar respuestas satisfactorias a los nuevos problemas que se plantean en el ámbito de Internet y las comunicaciones electrónicas.

Para el campo de análisis, estudiamos, en un primer momento, las expectativas de privacidad que tienen los usuarios con sus Isp, explicando bajo qué condiciones y supuestos se presentan (y creemos que se suscitarán) los mayores problemas. Luego, investigamos distintas hipótesis de riesgos que –estimamos- se plantearán en el futuro.

De este modo, hemos ido concluyendo algunas líneas de acción que podemos resumir brevemente en dos grupos de conclusiones, en nuestro primer grupo las generales, en el segundo, referidas más en detalles a los casos de estudio. Partamos con el primer grupo.

En las primeras páginas de este trabajo, fuimos desglosando conceptos para poder desarrollar lo que creemos puede conceptualizar al derecho al anonimato. A través de la evolución histórica y legal de derechos asociados, como la intimidad y la privacidad, llegamos a la definición del derecho al anonimato aplicado en las comunicaciones electrónicas, **como el derecho que tiene el usuario de Internet para que su identidad permanezca oculta o en forma reservada ante la mirada de otros actores que se desenvuelven en la red.**

De esta manera, concluimos, que el contenido del derecho al anonimato incluye la confidencialidad de las comunicaciones en Internet, la confidencialidad de los datos de tráfico y de todos aquellos datos e informaciones que permitirán al usuario actuar con la mayor libertad posible en la red. Así, el anonimato se presenta como necesario para el desenvolvimiento en la red.

Es entonces cuando surgen las implicancias del alcance jurídico de este nuevo concepto. A través de los estudios de caso presentados vimos que dichos efectos aún pueden ser difusos lo que nos lleva a nuestra segunda conclusión.

En efecto, el derecho al anonimato todavía no es unánimemente aceptado en materia jurisprudencial, por lo mismo puede carecer de la fuerza necesaria para una adecuada defensa de los intereses que el mismo derecho protege. En otras palabras, debido a la incipiente – y aún no cerrada – discusión acerca de la naturaleza jurídica del derecho del anonimato, será conveniente ceñirse a conceptos aceptados por la mayoría en el quehacer jurídico, como el derecho a la privacidad o intimidad a la hora de recurrir a nuestros tribunales por la defensa de nuestras garantías.

Pero éste no fue el único obstáculo en la aplicación empírica del derecho al anonimato. Así es como planteamos que el ser anónimo en Internet genera una serie de problemas.

Analizamos los casos donde el anonimato implica una dificultad para la detección de los autores de los delitos que se cometen en los medios informáticos. En este sentido, creemos que quedó en evidencia, que el límite del derecho al anonimato no es absoluto, y cederá en circunstancias que se protejan otros bienes jurídicos como es el caso de la persecución de ciertos delitos.

En este mismo contexto, advertimos que hay quienes consideran que el anonimato, junto con ser una garantía para la libertad de expresión, puede ser un fomento para la difusión de contenidos difamatorios o injuriosos, protegiendo la identidad de quienes realizan estas acciones so pretexto de cuidar su anonimato. Nosotros nos desmarcamos de algunas visiones que consideran a todos los usuarios de Internet como potenciales delincuentes, y que por lo tanto merman inútil y exageradamente la libertad en la red y el mismo derecho al anonimato. Al contrario, pensamos que el derecho al anonimato se sustenta precisamente en una garantía de las libertades cívicas que, como derecho esencial, presume la inocencia de las personas.

Es a raíz de esta situación que nos trasladamos a la otra esfera del desarrollo del anonimato; la regulación de la red para que las medidas protectoras de las libertades individuales se conjuguen perfectamente con la protección que el derecho debe brindar a la sociedad de los ilícitos que se cometen en sede virtual.

De este modo, apreciamos cómo en la regulación de la red se habla de diversos aspectos a ser considerados en función de hacer respetar el resguardo de las garantías fundamentales de los usuarios, tanto en el ámbito civil, como en el penal, desde la perspectiva del interés de la sociedad hasta el interés individual.

En este sentido, la regulación se ha visto desde distintos prismas. Por un lado, desde la acción estatal y la regulación de los ordenamientos jurídicos nacionales en conjunto o aisladamente. Analizamos los casos de Estados Unidos, de Europa y de nuestro país, que nos llevan a sacar lecciones acerca de cómo tratar el tema de la regulación y como la podemos aplicar al derecho del anonimato, para hacerlas compatibles, no sólo con nuestra visión de sociedad, sino que también con la visión integradora de la globalización.

Llegamos así a la noción de que la regulación no es lejana a la realidad, pero sí debe contemplar los diversos aspectos que hemos mencionado durante este trabajo. Por un lado, la acción estatal, que si bien es compleja, no es del todo ausente y, por el contrario, tiene, por el momento, el rol principal dentro de los cauces en los que se lleva a cabo la regulación en Internet, desplazando al rol que pueda jugar la autorregulación. Por otro, la autorregulación misma, que viene a suplir aquellas falencias que podrían o bien, dejar en la anarquía el mundo virtual, o bien, hacer de la red un estado policial.

Este nuevo marco de acción permite establecer una primera línea de equilibrio entre las garantías individuales y la protección a la sociedad. Parte de los mismos individuos hacia la comunidad. Sin embargo, este sistema, aunque ideal, no es siempre suficiente.

Menos preponderante será el rol que demos a la autorregulación en el ámbito penal. En este sentido, hemos de concluir que las medidas que se adoptan en miras de la persecución penal, devienen en una limitación al derecho del usuario a la privacidad. Los parámetros de estas restricciones a un derecho fundamental de los usuarios se discuten en Chile en sede legal en la ley 19.927, (la llamada Ley de Pedofília) en donde se imponen mandatos de control y registro a cargo de los ISP. Pasamos a nuestro quinto punto en este capítulo final.

En casos del ámbito penal, existe la idea de que controlando la demanda no exista oferta y, con ello, se acabe la producción y transmisión de material ilícito. Sin embargo, pensamos que esta opinión no toma en consideración la línea evolutiva que ha tenido la pornografía infantil, en cuanto ya no es claramente distinguible el fin comercial o de lucro, pues el gran problema hoy es el intercambio. De ahí que futuras revisiones a las restricciones en las comunicaciones deben apuntar en este sentido. Por lo mismo, la velada restricción al derecho al anonimato sólo debería ampliarse en el futuro en la medida que se reformulen estas hipótesis delictuales.

Como señalamos anteriormente, consideramos que toda regulación al respecto no debe tomar al usuario de Internet como el ser peligroso, como potencial delincuente al cual hay que controlar toda vez que el usuario de Internet se presente como un sujeto anónimo no es en sí mismo reprochable, y es más, se presenta, ese anonimato, como un derecho que debe ser tutelado por el ordenamiento jurídico.

Hemos dado un rol importante a la responsabilidad de los Prestadores de Servicios de Internet, que en el derecho comparado parecen seguir las mismas líneas de responsabilidad, que van de acuerdo a las necesidades operacionales de la red. Esto es, no dificultando la rapidez y eficiencia de los contenidos de la red, defendiendo, al mismo tiempo, los derechos de las personas, en la medida que los Prestadores tengan conocimiento de las infracciones.

En la medida que se vincula con ideas anteriores, ya que podríamos caer en la situación que los Prestadores de Servicios de Internet se convirtieran en verdaderos policías de la red. Si ya mencionamos que nos oponemos a un Estado policial en la red, con mayor razón rechazamos enérgicamente la idea que los ISP se conviertan en entes todos poderosos respecto al derecho del anonimato de los usuarios.

En cuanto a los datos personales que manejan los ISP, que pueden verse en colusión con la comisión de un delito, estimamos que es inviolable no sólo el mensaje, sino todos aquellos datos relativos a la comunicación que permitan identificar a los interlocutores o corresponsales, o constatar la existencia misma de la comunicación, su data, duración y todas las demás circunstancias concurrentes útiles para ubicar, en el espacio y en el tiempo, el hecho concreto de la conexión telemática producida, a menos que exista la adecuada autorización en sede jurisdiccional para realizarlo.

Cerrando estas primeras ideas, y a modo de resumen, señalamos que, para nuestra tesis resulta importante presenciar cómo, cada vez de forma más habitual, el anonimato se relaciona con conductas ilegales. El anonimato no es la fuente de la ilicitud en Internet. Los partidarios del anonimato no son potenciales delincuentes, sino sujetos que lo consideran como una garantía esencial, idea a la cual adscribimos, aun a pretexto de sonar reiterativos.

Ahora, corresponde el segundo grupo de conclusiones.

En primer lugar, y referido al impacto de Internet en la propiedad intelectual, para objeto de determinar cómo se ve afectada la privacidad, consideramos que el principal problema que se suscitará en los sistemas de regulación jurídicos guarda relación con una tendencia a criminalizar ciertos actos en la red, como el intercambio de contenidos a través de redes de p2p, concepto ya analizado en el cuerpo de este trabajo.

En segundo lugar, y en el caso del uso de datos necesarios para la entrega del servicio, (registros de facturación), a primera vista podría parecer que el usuario, debido al consentimiento que realiza con el prestador de servicio, no tiene una expectativa razonable de privacidad. Sin embargo, hemos concluido que debemos desechar esta perspectiva.

En tercer lugar, ligamos las problemáticas asociadas a la vulnerabilidad de la privacidad con un ámbito siempre conflictivo, como es el derecho laboral. Las hipótesis planteadas, respecto a la protección de la intimidad, reflejado en el anonimato en la red, deben contextualizarse en una relación de desigualdad de los sujetos.

Debemos tomar en cuenta que la autonomía privada se ve, por lo tanto, restringida en pos de la protección del trabajador. Si bien, no hay límites concretos para conocer cuándo y en qué momentos se deben proteger los derechos de manera especial,

cabe afirmar que sí podemos esperar una protección especial del derecho a la intimidad por los motivos antes dados. Por lo tanto, la futura jurisprudencia laboral debería tender a proteger el derecho al anonimato del trabajador frente a los intentos del empleador de conocer el contenido de sus comunicaciones electrónicas.

En cuarto término, afirmamos que el correo electrónico se encuentra protegido por la Carta Fundamental. El carácter de comunicación privada no depende de la propiedad de los equipos a través de los cuales se realiza.

La tecnología debe facilitar el acceso de las personas a los órganos de administración del Estado, y no restringirlo. La interoperabilidad es necesaria, pero no al costo de los derechos de las personas. Afirmamos la inconstitucionalidad del Decreto Supremo Nº 77, ya que establece mayores requisitos que los que establece la Constitución en su artículo 19 nº 14.

Antes de finalizar nuestras conclusiones quisiéramos sólo agregar unas palabras a modo de reflexión:

El anonimato no es un concepto cerrado sino que encierra una serie de posibilidades. Se presenta como el derecho que tiene una persona a la reserva su identidad ante la sociedad en Internet.

El anonimato es una garantía esencial para que la participación social en Internet pueda ser completamente libre. En la actualidad existe una pérdida de espacios anónimos, lo que nos parece muy peligroso. La corriente actual en legislación, política y tecnología es desconocer los beneficios del derecho al anonimato en la red. Los beneficios del anonimato en la red son los que se derivan de la libertad de expresión y el libre acceso a la cultura. En la vida real muchas de las relaciones sociales se efectúan en forma anónima y no se produce la fuerte crítica que se provoca en Internet.

El anonimato no puede ser contemplado como una herramienta individual, sino que debe potenciarse su cara social e institucional. El derecho al anonimato no está dirigido a los "especímenes raros" que navegan en la red, sino a cada uno de los usuarios de la red. No debe confundirse al anonimato con el aislamiento social.

El derecho al anonimato encuentra su justificación en permitir el libre desarrollo de la persona, que no es otra cosa que la posibilidad de elegir lo que uno puede hacer con su vida aplicado al ámbito de Internet. Su autonomía conceptual, con respecto a la privacidad, está dada porque los niveles de protección al usuario en uno y otro concepto difieren.

En el plano tecnológico, la implantación del ipv6 es necesaria, pero también lo es el respeto al anonimato del usuario. Se debe estudiar las repercusiones de la evolución de Internet sobre el anonimato.

Creemos necesario señalar que, así como se ha analizado en el presente estudio, más que leyes y normas jurídicas especificas y concretas, hay que tener en cuenta principios o directrices generales a través de los cuales se pueda dar una solución ágil y dinámica a un problema que, sin lugar a dudas, avanzará de la misma forma.

De esta forma, en el mundo globalizado si no se pone acento en la protección de las comunicaciones, derivaremos a un mundo en constante vigilancia y, además, paranoico al tratar a todos los usuarios de las nuevas tecnologías como sujetos peligroso y potenciales delincuentes. Lo anterior escapa, de cualquier forma, a los fines que el mismo derecho protege, y puede llevar a convertir a todo el ordenamiento jurídico en el peor enemigo de las garantías de las personas.

BIBLIOGRAFÍA.

1-Fuentes Doctrinarias:

BÉJAR, HELENA. “El ámbito íntimo. Privacidad, individualismo y modernidad”. Editorial Alianza . Madrid, España, 1988.

BRAVO LILLO, CRISTIÁN. “¿Que es interoperabilidad?”. En: http://www.kind.cl/kind/index2.php?option=com_content&do_pdf=1&id=9. 19 Septiembre 2006. (última visita 18 de Abril 2007).

BRUERA, Matilde y Bruera, Hugo. “Derecho Penal y garantías individuales: Registros penales y autoritarismo”. Editorial Juris. Rosario, Argentina, 1997.

CEA, JOSÉ LUIS. “El Derecho Constitucional a la Intimidad”. En: Revista Gaceta Jurídica Nº 194, Editorial Conosur, 1996.

CORRAL TALCIANI, HERNÁN. “Derechos al honor, vida privada e imagen y responsabilidad civil por los daños provocados por las empresas periodísticas”. En: Revista de Derecho, Universidad Católica de la Santísima Concepción, volumen V , Concepción, Chile,1994.

CASTELLS, MANUEL. “La Galaxia Internet”. Editorial Areté. Barcelona, 2001.

CASTELLS, MANUEL. “Internet, Libertad y Sociedad : Una perspectiva Analítica” . Lección inaugural del curso académico 2001-2002 de la UOC (Universitat Oberta de Catalunya). Publicado en http://www.uoc.edu/web/esp/launiversidad/inaugural01/intro_conc.html# . Última visita 2 de Junio 2005.

DE ANDRÉS BLASCO, JAVIER [et al.]; GARCÍA MEXÍA, PLABLO (director). “Principios de Derecho de Internet . Editorial Tirant Lo Blanch. Valencia, 2002.

DELPIAZO, CARLOS. “El nuevo Derecho en la Sociedad de la Información”. Edición Digital Actas del X congreso iberoamericano de informática y derecho. Santiago, Chile, Septiembre 2004.

NOUGRERES, ANA BRIAN. “El Spam: ¿Dis- Función de De-función de redes?”, Memorias del X Congreso Iberoamericano de Derecho e Informática. Ediciones Lom, Chile, 2004.

GARCÍA SAN MIGUEL, LUIS. “Estudios sobre el Derecho a la Intimidad”. Editorial Tecnos Universidad de Alcalá de Henares, Madrid, 1992.

FERNÁNDEZ PINÓS, JOSÉ ERNESTO [et al.]; MORALES PRATS, FERMÍN, [y] MORALES GARCÍA, ÓSCAR, (coordinadores). **“**Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet”. Editorial Aranzadi. Navarra, España, 2002.

Koenig, Christian, Ernst Röder and Sascha Loetz . “The Liability of Access Providers. A proposal for regulation based on the rules concerning access providers in Germany”. International Journal of Communication, Law and Policy. Issue 3, 1999. http://www.digital-law.net/IJCLP/3_1999/pdf/ijclp_webdoc_7_3_1999.pdf

LESSIG, LAWRANCE. “El Código y otras leyes del Ciberespacio”. Editorial Taurus Santillana. Madrid, 2001.

LESSIG, LAWRANCE. “La ley del caballo”. Programa Derecho y Tecnologías de la Información. Fundación Fernando Fueyo Laneri, Facultad de Derecho Universidad Diego Portales.
En: http://www.derecho.udp.cl/site/apuntes%5Cint%5Cla_ley_del_caballo_llessig.PDF
Última visita 2 Junio 2005.

LESSIG, LAWRANCE . “Cultura libre: cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad”. 2004. Publicado en http://cyber.law.harvard.edu/blogs/gems/ion/Culturalibre.pdf . (última visita 10 Junio 2006).

LÓPEZ MELGAREJO, ANTONIO. “Investigación Criminal y Proceso Penal: Las Directrices de la Propuesta del Consejo de Europa sobre Cyber-Crime y de la Directiva del Comercio electrónico”. En: Revista Derecho Procesal y Penal, número 8, Editorial Aranzadi, Navarra, 2002.

MAYANS I PLANELLS, JOAN. "Anonimato: el tesoro del internauta". En: Revista iWorld, Octubre, 2000. Publicado en http://www.cibersociedad.net/archivo/articulo.php?art=28, última visita 2 de Junio 2005.

MORALES, FERMÍN, “Pornografía infantil e Internet”. En: Jornadas de Responsabilidad Civil y Penal de los Prestadores de Servicios en Internet (Barcelona, 22-23 de noviembre de 2001). Publicado en http://www.uoc.edu/in3/dt/20056/index.html, (última visita 3 de Junio 2005).

MORÓN LERNA, ESTHER. “Internet y derecho penal: Hacking y otras conductas ilícitas en la red”. 2º Edición. Editorial Aranzadi, Navarra, 2002.

MIGUEL ASENCIO, PEDRO ALBERTO. “Derecho privado de Internet”. Editorial Civitas, Madrid, 2001.

MUÑOZ MACHADO, SANTIAGO. “La Regulación de la Red. Poder y Derecho en Internet”. Editorial Taurus, Madrid, 2002.

NOGUEIRA ALCALÁ, HUMBERTO. "El Derecho a la libertad de opinión e información y sus límites: honra y vida privada". Editorial LexisNexis. Santiago, Chile, 2002.

NOVOA MONREAL, EDUARDO. "Derecho a la vida privada y libertad de información: un conflicto de derechos". Editorial Siglo XXI. México, 1997.

NÚÑEZ ERRÁZURIZ , JAVIER. "La Autorregulación como Concepto Regulatorio." Documento de Trabajo Nº171, Departamento de Economía, Universidad de Chile, Santiago, 2000.

ORTEGA, ALFONSO. "El Derecho a la Protección de Datos de carácter personal en Internet". Memorias del X Congreso Iberoamericano de Derecho e Informática. Ediciones Lom, Chile, 2004.

ORTÍ VALLEJO, ANTONIO. "Derecho a la intimidad e informática". Editorial Comares, Granada , España, 1994.

PEÑA GONZÁLEZ, CARLOS. "El Derecho Civil en su relación con el derecho internacional de los derechos humanos". Cuadernos de Análisis Jurídico, Serie Publicaciones Especiales Nº 6 (Cecilia Medina y Jorge Mera editores). Universidad Diego Portales, Santiago, 1996.

PÉREZ LUÑO, ANTONIO. "Internet y Los Derechos Humanos". En: Revista Derecho y Conocimiento, Anuario Jurídico sobre la Sociedad de la Información, Volumen 2, Facultad de Derecho Universidad de Huelva. Publicado en http://www.uhu.es/derechoyconocimiento/DyC02/DYC002_A05.pdf, (última visita 3 Junio 2005).

PÉREZ LUÑO, ANTONIO. "Impactos sociales y Jurídicos de Internet, Argumentos de Razón Técnica". En: Revista española de Ciencia, Tecnología y Sociedad, y Filosofía de la Tecnología. Publicado en http://www.argumentos.us.es/numero1/bluno.htm , (última visita 3 de Junio 2005).

RETAMAL, JAIME. Boletín del Ministerio Público, N 20, Santiago, Chile, Septiembre 2004.

RIBAS, JAVIER ALEJANDRO. "Aspectos Jurídicos del comercio electrónico". Editorial Aranzadi. Pamplona, España, 1999.

SÁNCHEZ ALMEIDA, CARLOS. "De los Ciberderechos a la Ciberrevolución, presente y futuro de las libertades en la Internet española". En: http://www.bufetalmeida.com/ciberderechos.pdf, (última visita 1 Junio 2005)

SÁNCHEZ BRAVO, ALVARO. "Espionaje en el Ciberespacio". En: II Congreso Mundial de Derecho Informático, España; Cuna de un Mundo Global, Facultad de Derecho Universidad Complutense de Madrid, 23-27 de Septiembre de 2002, http://www.ieid.org/congreso/ponencias/Sanchez%20Bravo,%20Alvaro%20A.pdf
(última visita 3 de Junio 2005),

UGARTE CATALDO, JOSÉ LUIS. "El derecho a la intimidad y la relación laboral". Boletín Oficial Computacional Dirección del Trabajo. Año XII, número 39, Editorial Publitecsa, Santiago de Chile, Agosto 2000.

VERCELLI, ARIEL. "La conquista silenciosa del Ciberespacio". Publicado en http://www.arielvercelli.org/ . Buenos Aires , Argentina, Marzo 2004.

XALABARDER, RAQUEL. "Infracciones de Propiedad Intelectual y la Digital Milenium". En: "Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet", Editorial Aranzadi, 2002.

ZÚÑIGA, FRANCISCO. "El derecho a la intimidad y sus paradigmas". En: Revista Ius et Praxis, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, año 3, Nº 1, Talca , 1997.

Boletín de Derecho Autor, "El entorno numérico: La responsabilidad en materia de derecho autor", Ediciones UNESCO, Volumen XXXV, Nº 2, abril-Junio 2001.

Revista Jurídica Universidad de Puerto Rico, Volumen 72, Nº 4, año 2003.

Revista Chilena de Derecho Informático, Nº 3, Diciembre 2003.

Departamento de Estudios de la Defensoría Nacional penal. "Comentarios la Ley 19.927 de Delitos de Pornografía Infantil". En: http://www.defensoriapenal.cl/index.php?seccion=6&id=37, (última visita 15 Junio 2005).

2- Fuentes legales y jurisprudenciales:

Ley Nº 19.927. Modifica el Código Penal, Código de Procedimiento Penal y el Código Procesal Penal en materia de pornografía infantil.

Ley Nº 17.336 sobre Propiedad Intelectual.

Tratado Libre Comercio con EE.UU. Capítulo Quince sobre comercio electrónico y capítulo diecisiete sobre Derechos de propiedad intelectual.

Ley N° 19.628 sobre Protección de la vida Privada.

Resolución Exenta Nº 1.483 que fija procedimiento y plazo para establecer y aceptar conexiones entre ISP.

Ley Nº 18.168 General de Telecomunicaciones.

Proyecto de Ley sobre Comunicaciones electrónicas. (Boletín Nº 2512-07).

Proyecto de Ley sobre Responsabilidad por los contenidos de Internet. (Boletín Nº 3004-19.)

Proyecto de ley sobre comercialización y publicidad por medio de redes de telecomunicaciones e Internet. (Boletín Nº 3094-19).

Decreto Supremo Nº 77, del Ministerio General de la Presidencia, que aprobó la normativa técnica sobre la eficiencia de las comunicaciones electrónicas entre Órganos de la Administración del Estado y entre éstos y los ciudadanos, de 23 Diciembre 2004.

Decreto Supremo N° 81, del Ministerio Secretaria General de la Presidencia, que aprobó la normativa técnica para los órganos de la Administración del Estado sobre interoperabilidad de Documentos Electrónicos, de 23 Diciembre 2004.

Decreto Supremo Nº 83, que aprueba una norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, 12 Enero 2006.

Oficio Nº 118, del Ministerio Secretaria General de la Presidencia, referente al Decreto Supremo Nº 81 y Oficio Nº 1360 del Ministerio del Interior referente al Decreto Supremo Nº 83.

Sentencia de 6 de diciembre 2001 recaída Recurso protección Ustovic Kaflick, Izet y otra con Saez Infante, Eugenio y otros. Corte Suprema, 30 enero 2002, ingreso Nº 127-02

Sentencia de 6 de diciembre de 1999 de la Iltma. Corte de Apelaciones de Concepción recaída en el Recurso de Protección interpuesto por Orlando Fuentes Siade contra ENTEL S.A., ingreso Nº 243-99.

Sentencia de 21 de marzo de 2003 de la Iltma. Corte de Apelaciones de Puerto Montt recaída en el Recurso de Protección interpuesto por Patricio Navarro Silva contra el portal KAPSULA.CL, ingreso Nº 3.718.

3-Derecho Comparado.

Convenio sobre la Ciberdelicuencia del Consejo de Europa. Budapest, 23 Noviembre .2001. Publicado en https://www.gdt.guardiacivil.es/media/Convenio_Ciberdelincuencia.pdf

DIRECTIVA 2000/31/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). DOCE L 178 de 17.07.2000

DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). DOCE N° L 201 de 31.07.2002

Ley Española 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Publicada en el Boletín Oficial del Estado Nº 166 de 12 de julio de 2002. España

Ley Española 32/2003, de 3 de noviembre, General de Telecomunicaciones. Publicada en el Boletín Oficial del Estado 04 noviembre de 2003.

Decisión Nº 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. DOCE N° L 033 de 06.02.1999

Decisión Nº 1151/2003/CE del Parlamento Europeo y del Consejo, de 16 de junio de 2003, que modifica la Decisión nº 276/1999/CE por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales. DOCE L 162 de 01.07.2003, página 1.

Resolución del Consejo de 28 de enero de 2002 relativa a un enfoque común y a acciones específicas en materia de seguridad de las redes y de la información. DOCE N° C 043 de 16.02.2002, página 2.