Papeles el tiempo de los derechos

INTERNET, ENTRE LA SEGURIDAD Y LOS DERECHOS HUMANOS. NECESIDADES DE REGULACIÓN

Ruiz-Morales, Manuel L.
Universidad de Cádiz

Palabras clave: Intimidad. Libertad de expresión. Control social. Seguridad. Internet.

Número: 7 Año: 2016

ISSN: 1989-8797

Comité Evaluador de los Working Papers “El Tiempo de los Derechos”

María José Añón (Universidad de Valencia)
María del Carmen Barranco (Universidad Carlos III)
María José Bernuz (Universidad de Zaragoza)
Manuel Calvo García (Universidad de Zaragoza)
Rafael de Asís (Universidad Carlos III)
Eusebio Fernández (Universidad Carlos III)
Andrés García Inda (Universidad de Zaragoza)
Cristina García Pascual (Universidad de Valencia)
Isabel Garrido (Universidad de Alcalá)
María José González Ordovás (Universidad de Zaragoza)
Jesús Ignacio Martínez García (Universidad of Cantabria)
Antonio E Pérez Luño (Universidad de Sevilla)
Miguel Revenga (Universidad de Cádiz)
Maria Eugenia Rodríguez Palop (Universidad Carlos III)
Eduardo Ruiz Vieytez (Universidad de Deusto)
Jaume Saura (Instituto de Derechos Humanos de Cataluña)

INTERNET, ENTRE LA SEGURIDAD Y LOS DERECHOS HUMANOS. NECESIDADES DE REGULACIÓN.

Ruiz-Morales, Manuel L.[1]
Universidad de Cádiz

I. INTRODUCCIÓN

Desde hace ya varias décadas Internet se ha ido convirtiendo en una herramienta indispensable para cualquier persona en el mundo actual, debido principalmente a los avances que se fueron produciendo en el ámbito tecnológico desde mediados del siglo pasado hasta la actualidad.

La información y la comunicación fueron ámbitos en los que se pudo apreciar ese desarrollo exponencial de la técnica, máxime con la aparición de la informática y, a partir de finales del siglo XX, de Internet, lo que ha dado lugar a la denominada "sociedad de la información[2]".

Esta nueva forma de sociedad en la que el hombre interactúa con sus semejantes con cualquier finalidad, requiere en la operatividad habitual y cotidiana de la utilización de medios de comunicación electrónicos interconectados, que posibilitan el contacto y acercamiento de personas situadas a miles de kilómetros, reduciéndose considerablemente el tamaño del planeta, lo que ha dado lugar a la era de la globalización, u "hogar global[3]".

Estas nuevas formas de relacionarse han provocado innumerables cambios y modificaciones sociales. Por mencionar algunas de éstas, se puede destacar las habidas a la hora de contactar con otras personas (como son las reglas de cortesía), las producidas en las formas de educar (ocupando un papel relevante las plataformas de *e-learning*), las prácticas de tele-democracia o votación a través de la red, el establecimiento de nuevas relaciones de amistad o de pareja de sujetos hallados en lugares geográficos distantes o, incluso, la aparición en el seno de la sociedad de desconocidas enfermedades (como las

[1] Doctorando en Derecho Penal por la Universidad de Cádiz. Investigador invitado en el Instituto de Investigaciones Jurídicas y Sociológicas Ambrosio L. Gioja, de la Facultad de Derecho de la Universidad de Buenos Aires.

[2] C. C. SUEIRO, "La criminalidad informática en el Anteproyecto de Código Penal de la Nación", *Revista Derecho Penal,* núm 7, 2014, pp. 189-191.

[3] A. E. PÉREZ LUÑO, "Internet y los derechos humanos", *Anuario de Derechos Humanos, Nueva Época*, núm 12, 2011, pp. 291-292.

ludopatías de la red o ciberadicciones, que surgen como resultado de la sobreexposición a la información)[4].

Igualmente, como se viene explicando, estos efectos producidos por la "sociedad de la información" son posibles gracias a Internet. El potencial uso de esa red global trastoca aspectos sustanciales también en el ámbito económico y político, ya que ha posibilitado una nueva forma de entender la economía, puesto que la productividad de las empresas y la competitividad de dichos agentes, dependerán de las capacidades de gestión, procesamiento y utilización de cantidades ingentes de información; impulsando otros campos a partir de éste, como el político, el jurídico, el asistencial, el mercantil o el transaccional, ya que todos encuentran enclave dentro de esta red internacional[5].

Como consecuencia, se trata del foro idóneo para ejercer de una manera absoluta un derecho fundamental, como es el caso particular de la libertad de expresión. De este modo, a partir de este declarado derecho humano, cada persona puede realizar las investigaciones que estime pertinentes y comunicar o publicar las informaciones que desee de cualquier manera, esto es, a través de cualquier medio, con el límite de no violentar los derechos humanos de otros sujetos[6]. Por tanto, Internet ofrece una incondicional capacidad de transmitir alguna información, averiguaciones o las propias opiniones, de cualquier índole, ya sean científicas, políticas, religiosas, etc. Ahora bien, lo más relevante es la circunstancia de permitir la expansión de esa divulgación a cualquier parte del mundo, a cada dispositivo que se encuentre conectado a la red.

Lógicamente, ese espacio de libertad también es aprovechado por ciertas personas o grupos de personas, para efectuar actividades delictivas, dando lugar a lo que se conoce como ciberdelincuencia. Esta modalidad ilícita se desenvuelve habitualmente en torno a organizaciones criminales, del campo del narcotráfico, terrorismo, tráfico de armas, trata de blancas, tráfico de órganos, inmigración ilegal de personas, falsificación, prostitución, fraudes, entre otras, bajo el parapeto del anonimato que ofrece Internet, puesto que aunque el internauta siempre deja un rastro en la red, la misma puede camuflarse, disiparse, haciendo muy complicado el descubrimiento, la prueba y la

[4] A. ESTRADA CUZCANO, "Internet: cambio social, libertad e intimidad", *Escritura y Pensamiento*, núm 16, 2005, pp.151-152.

[5] M. CASTELLS, *La era de la información: la sociedad red*, Alianza Editorial, 2ª Ed., Madrid, 2001, pp. 489.

[6] C. CASTILLA JUÁREZ, *Libertad de expresión y Derecho de Acceso a la Información en el Sistema Interamericano de Derechos Humanos*, Comisión Nacional de los Derechos Humanos, México, 2011, pp. 27.

persecución del delito[7], máxime cuando el autor puede situarse en el territorio de un Estado ubicado al otro extremo del orbe[8].

Ante esta tesitura, los estados nacionales se encuentran ante un silogismo u argumento cornuto, toda vez que necesitan de esta red internacional para garantizar libertades personales y empresariales, favorecer la educación, incitar el desarrollo económico y social; no obstante, a través de este medio se deja penetrar una importante amenaza: la del crimen y la delincuencia, la del descontrol y la del desorden; por ello, ante la observancia de verse perjudicado en sus intereses, el Estado intenta controlar (en mayor o menor medida) Internet[9].

Y es que Internet funciona como el cuerpo humano. De este modo, cada individuo, cada usuario a través de su ordenador o smartphone actúa como si fuese una célula. Así, esta célula, este internauta, no es más importante que otro distinto individualmente considerado. Ahora bien, cada célula o tipo de células cumplen una funcionalidad, al igual que cada usuario de internet usa esta herramienta con una finalidad diversa (y existen grupos de internautas con similares patrones de actuación en la red). Pues bien, los Estados actúan como si fueran los órganos del cuerpo, que intentan mantener el funcionamiento normal del mismo, por ello opera a través de la vigilancia, observando y comprobando si en su interior se ha producido algún incidente, piénsese herida, hemorragia, o alguna célula se ha tumorizado en el interior del cuerpo humano. Lo mismo es trasladable a la vida en Internet, toda vez que el Estado controla si existen personas molestas con el sistema, vigila que todo esté en orden, intenta paliar eventuales perturbaciones, e incluso restablece la situación si a pesar de todo se produjo un desbarajuste, a través de la comisión de un ilícito.

El problema de esta supervisión se halla en rebasar ciertos límites constitucionales. Este es el nudo gordiano del presente artículo, analizar las formas de vigilancia y control del Estado a través de Internet, específicamente, aquellas formas que conllevan la vulneración de ciertas libertades fundamentales, como es el caso de la libertad de expresión y el derecho a la intimidad, debido principalmente a la prevalencia que hace el Estado de sus actuaciones, no sólo cuando se trate de regímenes totalitarios, sino también en los denominados sistemas democráticos. Una vez cumplida sucintamente esta pretensión, se aportarán herramientas necesarias para salvaguardar estos derechos

[7] A. E. PÉREZ LUÑO, "Internet y los derechos humanos", *cit.*, pp. 295.
[8] Piénsese en la utilización por parte del Crimen Organizado Mundial de la llamada "deep web".
[9] A. L. RUBIO MORAGA, "Censura en la red. Restricciones a la libertad de expresión en Internet", en VV.AA., *Prensa y periodismo especializado II,* Guadalajara, 2004, pp. 597.

humanos de los ciudadanos en cualquier Estado, sin que pueda hacerse valer pretexto alguno en el menoscabo de esta tutela obligatoria, puesto que la protección de tan básicos derechos de las personas es vital a la hora de asegurar un espacio o esfera moral de libertad, sin ni siquiera permitirse injerencias gubernativas o estatales, más aún cuando son de naturaleza subrepticias (al saberse ilegales), puesto que debido a la preeminente posición estatal, éste ante incumplimientos de normas elementales, no se auto-infligirá castigo alguno (es más, habitualmente, ni se instruirá esa posible vulneración por parte de los miembros operativos del Estado).

II. ACCESO A INTERNET, LIBERTAD DE EXPRESIÓN Y CENSURA

En la actualidad, aseverar que el acceso a Internet es un derecho humano no es algo nada extraño de escuchar, no obstante, no es que se trate de un derecho propiamente dicho, sino que se estipula como de tal categoría en tanto en cuanto la entrada a mencionada red informática global posibilita y favorece el ejercicio de los derechos humanos de una manera más plena, fundamentalmente los relativos a las libertades de expresión, opinión o asociación, puesto que Internet constituye un medio idóneo para manifestar pensamientos o reflexiones individuales, a la vez que permite proponer y exteriorizar posiciones y reivindicaciones colectivas o grupales.

En este sentido, en la sociedad actual globalizada, donde el flujo de ideas, noticias, conocimientos, sucesos, azota constantemente y diariamente a las personas, el acceder a mencionada información se configura como un derecho, puesto que se trata de una condición necesaria para la prosperidad[10].

Por tanto, en la medida en que estos derechos universales, inalienables e indivisibles se encuentran reconocidos en la Declaración Universal de los Derechos Humanos[11] (1948)[12], estos pueden y deben ser ejercitados libremente, sin ningún tipo de

[10] Véase el Detalle de la Comunicaciones de Prensa de la Comisión Europea, *"La Comisión hace un llamamiento en favor de una sociedad digital que no excluya a nadie"*, de 29 de Noviembre de 2007, en Bruselas (IP/07/1804), donde se manifestó tal postura.

[11] En adelante, DUDH.

[12] Art. 19: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

coartaciones o restricciones, ya vengan por parte del Estado o de entidades de índole privada[13].

Igualmente, estos derechos son tan esenciales para permitir el desarrollo del individuo que son acatados en multitud de textos internacionales con vinculación interna en los acervos jurídicos particulares de los diversos Estados. A título de mención, es destacable su consagración en el Pacto Internacional de Derechos Civiles y Políticos (1966) o la Convención Americana de los Derechos Humanos[14] (1969), entre otros.

De la misma manera, los textos constitucionales de la mayoría de los países del planeta, recogen también la tutela de estos fundamentales derechos. Y la utilización de Internet debe entenderse incluido dentro del "derecho a la información", ya que "*si un principio básico del derecho a la información es la universalidad, en el sentido de que este derecho fundamental de la comunicación libre se ejerce en cualquier lugar y por cualquier medio de comunicación, éste debe poder aplicarse a los medios con los que se puede y/o quiere recibir, acceder o difundir información*[15]", ningún medio de comunicación presenta tanto vigor para conectar personas y compartir información como Internet.

Evidentemente, ello no significa que el ámbito de actuación del sujeto a la hora de ejercitar la libertad de expresión sea irrestricto, ya que a la hora de verter opiniones, de expresar ideas o sentimientos, manifestar y comunicar informaciones, existen ciertos límites que el ser humano debe respetar, que vienen marcados por los derechos humanos de terceras personas y por la tutela del orden público y la seguridad nacional, esto es, razones personales y sociales, respectivamente[16].

Ahora bien, bajo ese tipo de argucias, esto es, so pretexto de estas zonas externas a la libertad de expresión, pensamiento e información, no debe permitirse actividades atentatorias contra estos derechos, algunas de ellas, propias de Estados y gobiernos totalitarios, mas muchas otras, llevadas a cabo por los sistemas adalid de los principios democráticos, que se jactan de disfrutar de regímenes plenamente garantistas.

---

[13] En tal sentido analizar la posición de la UNESCO al respecto. Véase en < http://www.unesco.org/new/es/communication-and-information/freedom-of-expression/freedom-of-expression-on-the-internet/>.

[14] En adelante, CADH.

[15] L. CORREDOIRA Y ALFONSO, "El derecho de acceso a la información en Internet", en *Actualidad Informática*, núm 32, 1999, pp. 1.

[16] L. E. CÁZARES ROSALES, "Los derechos a la intimidad, a la propia imagen y al honor vulnerados por el ejercicio abusivo de la libertad de expresión en Facebook", en *Nueva Época*, núm 17, 2014, pp. 45-46.

En primer lugar, como una gravísima violación de la libertad de expresión en su faceta de divulgación a través de la red informática de computadoras, se puede mencionar las prácticas prohibitorias del acceso a Internet existentes en algunos países, como Corea del Norte, en la Afganistán talibán. Esta forma es típica de los sistemas políticos dictatoriales, que presentan gran temeridad ante la información que circula libremente por Internet[17].

No obstante, en segundo término, se puede mencionar multitud de maniobras realizadas por Estados más o menos democráticos, como pueden ser: el acceso a la red controlado mediante concesiones de autorizaciones concretas para determinadas personas o fines; la monitorización o vigilancia de los contenidos publicados y visitados por los usuarios de Internet[18]; el bloqueo de sitios web inofensivos, pero políticamente "incómodos" para el gobierno de turno; o la fijación de leyes restrictivas de los derechos de los ciudadanos, que facilitan el control.

Todos estos supuestos son formas de censura encubierta, que consiguen silenciar determinadas ideas. Ahora bien, la CADH expresa que la libertad de expresión no puede estar sometida a una censura previa, sino que ésta debe operar posteriormente (sin menoscabo, además, de incurrir en ciertas responsabilidades), siempre y cuando vengan dispuestas por una ley (para tal supuesto), y si en virtud de una ponderación en el particular supuesto resultaren lesionados los límites personales y sociales[19] que se mencionaron *ad supra*.

Por último, es dable destacar también en este punto, un extracto de la primera sentencia que trató el tema de la censura en Internet, y que tuvo lugar en Estados Unidos. Decía así[20]: "*de acuerdo con la tradición constitucional de nuestro país, en ausencia de prueba en contrario, debemos presumir que la regulación de los contenidos y de la expresión está más cerca de interferir el libre intercambio de las ideas que de promoverlo. El interés de promover la libertad de expresión en una sociedad democrática está por encima de los beneficios teóricos e indemostrables de la censura[21]*".

---

[17] A. L. RUBIO MORAGA, "Censura en la red. Restricciones a la libertad de expresión en Internet", *cit*., pp. 599-600.

[18] Sobre este punto se prestará una mayor atención posteriormente, cuando se realiza de manera ilegal y afecta a los derechos humanos de los individuos.

[19] C. CASTILLA JUÁREZ, *Libertad de expresión y Derecho de Acceso a la Información*, *cit*., pp. 38.

[20] A pesar de la siguiente afirmación, se verá que Estados Unidos es uno de los países que más vulnera los Derechos Humanos a través del uso de Internet.

[21] Sentencia de la Corte Suprema de EE.UU., de 26 de junio de 1997.

III. EL DERECHO A LA INTIMIDAD Y SU VULNERACIÓN POR PARTE DEL ESTADO A TRAVÉS DE INTERNET

El derecho a la intimidad, por su parte, comienza a resonar en la época del liberalismo democrático[22], a través de las posturas de autores como Hobbes, Locke o Stuart Mill, quienes veían la necesidad de que el ciudadano particular tuviera un margen de independencia de una parte de su vida (la privada e íntima) alejada de la vida pública, esto es, de la actividad del Estado[23].

Sin embargo, no será hasta la mitad del siglo pasado cuando este derecho recibe acogida internacional, disfrutando a partir de entonces de una superior protección, por medio de su prescripción en el art. 12 de la DUDH[24], en el art. 8 de la Convención Europea de los Derechos Humanos, o en el art. 11 de la CADH. Igualmente, las Constituciones del mundo también reconocen este derecho como un derecho fundamental. En nuestro caso, la Constitución Española lo hace en su precepto número 18, agrupando en mencionado artículo, derecho al honor, a la intimidad y a la propia imagen, la inviolabilidad del domicilio y el secreto de las comunicaciones; haciendo especial referencia su apartado 4 al uso restrictivo de la informática en relación a tales garantías constitucionales[25].

Este derecho personalísimo, comprende un espacio de la vida individual y familiar, que debe quedar libre de la injerencia de cualquier tercero, y que permite desarrollar firmemente la personalidad, la identidad y la dignidad del individuo, abarcando también a las prerrogativas que facultan el control de la utilización que otros hacen de la información sobre sí mismo, esto es, sobre su persona[26].

Obviamente, este derecho también puede ser objeto de limitación, como declara la Sentencia del Tribunal Supremo de 28 de octubre de1986 al manifestar que "*queda encomendada al juzgador la prudente determinación del ámbito de la protección […] para trazar los límites de la intimidad*", en atención a las circunstancias del caso, el

---

[22] O incluso antes. Como reza la Sentencia de la Corte Suprema de Estados Unidos de 7 de junio de 1965, en el caso "Griswold v. Connecticut", el derecho a la intimidad es "*más viejo que la Declaración de Derechos, más viejo que nuestros partidos políticos, y más viejo que nuestro sistema escolar*".

[23] H. BÉJAR, *El ámbito íntimo. Privacidad, individualismo y modernidad*, Alianza Editorial, Madrid, 1990, pp. 45 y ss.

[24] Art. 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

[25] Art. 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". A pesar de esta precisión, se analizará como es el propio Estado el que vulnera estos derechos fundamentales de los ciudadanos.

[26] M. C. SABATER, "Vida de cristal. Análisis del derecho a la intimidad en la sociedad de la información", en *Intersticios. Revista Sociológica de Pensamiento Crítico*, núm 2, 2008, pp. 45-46.

momento, los usos de la sociedad, el cuidado de la intimidad por el propio interesado, el interés público del desvelo o investigación, entre otros aspectos.

Pues bien, respecto de lo dicho, Internet es una red de libre acceso, donde circula cualquier tipo de información, que permite ejercer plenamente la libertad de expresión. No obstante, como se comentó *ad supra*, Internet no es la panacea que permite un desarrollo absoluto del sistema democrático y de los derechos humanos, sino que, por el contrario, es un espacio propicio para la eclosión y la entronización de la delincuencia por sus características propias e inherentes relativas principalmente a su nula o escasa regulación, a la deslocalización de usuarios, a la imposibilidad de perseguir delitos fuera de las fronteras estatales donde puede estar actuando el autor del ilícito, entre otros problemas derivados que pueden afectar a derechos de los individuos y a bienes jurídicos fundamentales. Por tanto, estos supuestos constituyen peligros eminentes y paladinos para la mayoría de los ciudadanos que hacen uso de la red informática, en mayor o menor medida[27].

Ahora bien, prevaliéndose de esta situación y bajo el pretexto de la seguridad nacional, esto es, de encabezar la lucha frente a ciertos tipos de criminalidad que provocan una gran conmoción y altas cotas de alarma social (como es el caso de la pornografía infantil y el terrorismo) se están permitiendo y aceptando por la ciudadanía, leyes restrictivas de los derechos humanos (fundamentalmente a partir de los acontecimientos que cumplieron hace unos días su décimo quinto aniversario, es decir, los atentados del 11-S). Hasta tal punto que el Estado obtiene el beneplácito para ejercer una vigilancia y un control social exhaustivo de todos sus habitantes[28] y de los nacionales de otros países[29], vulnerando incluso los aspectos más personales e íntimos del sujeto y, en definitiva, poniendo en riesgo las libertades cívicas. Algunos autores han llamado a este

[27] E. GARZÓN VALDÉS, "Optimismo y pesimismo en la democracia", en *Claves de Razón Práctica*, núm 131, 2003, pp. 32.

[28] Incluso algunos autores manifiestan que Internet opera como Panóptico y Sinóptico, puesto que además de vigilar, propone y seduce valores y modelos de comportamiento. Igualmente, el potencial de la red es insoslayable, toda vez que no sólo permite supervisar, sino que siguiendo el rastro que se deja registrado el usuario, por las distintas webs, se puede construir y reconstruir las acciones de los internautas, observando antes de que se produzcan aquellos comportamientos potencialmente sospechosos, y en torno a él encasillar al sujeto, con la finalidad de llevar a cabo políticas de prevención y represión (*Banóptico*). Vid. M. RAGNEDDA, "Internet y control social. Entre Rizoma y Gran Hermano", en *Perspectivas de la Comunicación*, v. 4, núm 1, 2011, pp. 44-47.

[29] Piénsese en la estadounidense "*Patriot Act*".

fenómeno "*el fin de la privacidad*" o la "*infovigilancia*", al modo del "*Gran Hermano*" de Orwell, mas en una sociedad demócrata[30].

Las prácticas que dudosamente cumplen con las garantías constitucionales básicas que todo ser humano debe poseer, se caracterizan por la variedad. A veces, consiste en la interceptación de las comunicaciones y su registro con software creados para el efecto y que se apoderan de la información intercambiada, independientemente del lugar del mundo que se halle el sujeto. Con tal finalidad, los Estados cuentan con Servicios de Inteligencia o Agencias de Seguridad[31], e igualmente, con sistemas informáticos como *Echelon* o *Carnivore*, que siendo capaces de interceptar ilegalmente todo tipo de comunicaciones (sin ni siquiera requerir de autorización judicial), permite acceder a cantidad de información[32]; lo que la convierte en una de las tecnologías básicas empleadas actualmente en el espionaje, para la anticipación discreta de cualquier actuación contraria al gobierno[33], aún cuando no exista ni una mera sospecha o posibilidad inminente de un verdadero ataque a la seguridad nacional.

Igualmente, las empresas tecnológicas[34], los proveedores de Internet, las empresas de publicidad, las páginas web o redes sociales acumulan una cantidad incalculable de información personal, tanto facilitada por el usuario de la web, como la que se puede esgrimir de la interactuación del sujeto con la página electrónica[35]. Es el caso de fotos, amistades, amigos, lugares en los que se ha estado, etc. (usados por estas entidades con la finalidad de obtener beneficios de ella) y, que posteriormente, pueden llegar fácilmente a las autoridades encargadas de la seguridad estatal, de la categoría que fuere[36].

Pero la información obtenida así, no sólo comprende a los mensajes o al contenido de conversaciones, sino que también utilizan otra forma de someter a los individuos al control. Esa manera se ejecuta siguiendo el rastro dejado por los cibernautas en la red,

---

[30] R. WHITAKER, *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*, Paidós, Barcelona, 1999, pp. 101-169.

[31] VV.AA. "El control del ciberespacio por parte de gobiernos y empresas", en *Cuaderno Red de Cátedras Telefónica*, núm 9, 2012, pp. 15-17.

[32] Véase A. ESTRADA CUZCANO, "Internet: cambio social, libertad e intimidad", *cit.,* pp.160-161; y A. L. RUBIO MORAGA, "Censura en la red. Restricciones a la libertad de expresión en Internet", *cit*., pp. 604.

[33] Actuando como una policía del pensamiento (Thought-Police) que todo lo sabe.

[34] Algunas de ellas también se consideran empresas de la interceptación y la vigilancia, es el caso de Alcatel, ZTE Corporation o Huawei, (dependiendo de cada país), entre otras muchas.

[35] A cuyos derechos el usuario renuncia a la hora de la aceptar las políticas de privacidad, ya que todas las informaciones pasa a considerarse propiedad de esos operadores.

[36] D. RAYMAN LABRÍN, "Chile: Vigilancia y derecho a la privacidad en Internet", en *Revista Chilena de Derecho y Tecnología*, v. 4, num 1, 2015, pp. 204.

en la forma de micro-archivos o "*cookies*", que recrean la senda de la navegación. Éstas se utilizan para reconstruir el camino realizado en Internet, permitiendo la obtención del perfil del internauta[37]. En ese sentido, el control de los "metadatos" puede servir incluso de una mejor forma a los objetivos estatales de vigilancia, puesto que estos datos asociados a las comunicaciones, si bien no cuentan con el contenido, si proporciona aspectos tales como asiduidad, frecuencia, identidad de las mismas. Además, su facilidad de análisis y su aplicación son destacables, ya que a diferencia del fondo del asunto (piénsese en una llamada de teléfono), los metadatos son matemáticos y, por ello, precisos y susceptibles de empleo en operaciones analíticas, en un lenguaje universal[38].

Como consecuencia, ha surgido también el derecho a la autodeterminación informativa o *habeas data*, consistente en las prerrogativas de las que disponen las personas, a efectos de evitar abusos informáticos, almacenaje o uso desmedido de información personal[39].

En ese sentido, existe jurisprudencia reciente de Tribunales de diversos países, que explicitan supuestos aplicables en este punto. En Estados Unidos, se ha producido una diferenciación entre información de contenido (de la comunicación) y de no contenido. Por tanto, aquella que sea de contenido puede gozar de una mayor protección en base a la intimidad garantizada en la Cuarta Enmienda a la Constitución estadounidense. No obstante, la de no contenido puede ser empleada y requerida por el gobierno a los poseedores de tales informaciones, sin ni siquiera necesitar de autorización judicial al efecto, ya que la doctrina jurisprudencial entiende que cuando una persona revela información íntima a un tercero, asume el riesgo de que tal información sea comunicada posteriormente a la autoridad gubernamental, perdiéndose la esperanza de que se resguarde la intimidad[40].

En el mismo sentido, en relación a la transferencia de datos, el Tribunal Constitucional español ha manifestado que el derecho a la protección de los datos es un derecho fundamental, incluso independiente y rebasador del derecho a la intimidad. Por lo que esa transferencia de información sería muy limitada si no se cuenta con el

[37] A. ESTRADA CUZCANO, "Internet: cambio social, libertad e intimidad", *cit.,* pp.160-161.
[38] G. GREENWALD, *Snowden. Sin un lugar donde esconderse*, Ediciones B, Barcelona, 2014, pp. 165-167.
[39] L. E. CÁZARES ROSALES, "Los derechos a la intimidad", *cit.,* pp. 49.
[40] Sentencias de la Corte Suprema de EE. UU." Katz v. United States"; "United States v. Miller"; o "Smith v. Maryland".

consentimiento de los afectados[41], aunque sí se salvaguarda el Estado la posibilidad de obtenerlos en base al posible atentado a la seguridad estatal o a la persecución de infracciones penales.

Por otra parte, el Tribunal Supremo español[42] diferencia en dos tipos la información facilitada a las redes sociales, a saber: primero, los datos que forman parte del perfil público del sujeto, denominados accesibles; y en segundo lugar, los que se suministran a la empresa que gestiona la red social, que se conocen como no accesibles. Estos recibirían una protección mayor.

Ahora bien, este mismo Tribunal declaró recientemente que las Fuerzas y Cuerpos de Seguridad con el objeto de prevenir la comisión de ilícitos, puede vigilar los sitios públicos, incluidas las redes sociales (aunque se refiere a las manifestaciones públicas). Lo que no podrían hacer es intervenir las comunicaciones privadas[43]. No obstante, si un sujeto realiza una publicación en una red social y ésta sólo es compartida y visible entre sus contactos, ¿no debería entenderse que se hallan sólo habilitados para usar esa información los sujetos autorizados y sobre los que ha recaído expresamente tal aprobación al consentir el interesado su incorporación como amigo o seguidor?

Por su parte, también, en el 2015 se produjo la reforma de la Ley de Enjuiciamiento Criminal española, de fortalecimiento de las garantías procesales y de regulación de las medidas de investigación tecnológica, que, sin pronunciarse sobre los supuestos de espionaje estatal[44], obliga a los prestadores de servicios de telecomunicaciones o que realicen alguna contribución a facilitar las comunicaciones, a prestar colaboración, asistencia y deber de secreto en la investigación judicial[45].

IV. LA ACOTACIÓN DE LOS DESMANES EN EL CONTROL

De acuerdo a las premisas establecidas en el propio Convenio sobre Ciberdelincuencia de Budapest de 2001, se declara que incluso en la persecución de la delincuencia informática, es decir, en los delitos objeto de tipificación en virtud del propio Convenio, se deberán establecer condiciones y salvaguardas en el derecho interno de cada Estado, para, de este modo, proteger y tutelar los derechos humanos y las libertades

[41] STC 292/2000, de 30 de noviembre.
[42] STS de 31 de octubre de 2000.
[43] STS de 18 de julio de 2016.
[44] Puesto que dichas procedimientos son encubiertos y clandestinos, por lo que ni siquiera se reconoce su existencia.
[45] Art. 588 ter e.

fundamentales básicas contenidos en los principales textos internacionales que propugnan los derechos más básicos de las personas.

No obstante, como se ha venido comentando, los estados se preocupan más por salvaguardar la seguridad que por garantizar la libertad, lo que atenta contra los derechos esenciales de las personas, especialmente si la vigilancia estatal se realiza cumpliendo tres requisitos: Primero, recopilar información y datos que los propios internautas facilitan por cualquier medio telemático. Segundo, dirigirse a grandes grupos de usuarios, es decir, casi a la totalidad de la población masivamente, esto es, realizarse de forma sistemática, constante y monitorizada. Tercero, Usarlos para establecer gustos, preferencias, lugares de encuentro, asiduidad, frecuencia en realizar actos, conductas, pasatiempos, que sirven para identificar e individualizar a cada cibernauta, a través de datos que realmente no pensaban facilitar a la maquinaria estatal[46], eliminando toda presunción de inocencia en la ciudadanía, toda vez que el sistema pasa a basarse en el principio de culpabilidad.

De ahí que sea menester legislar en esta materia, tanto en el fuero de cada ordenamiento jurídico particular como en los fueros internacionales, con la finalidad de evitar esta supervisión intensiva, ya que de esta manera, en base a la ponderación en la limitación de los derechos humanos, las interpretaciones jurisprudenciales están siendo desmedidas, sin necesidad de argumentar y cumplimentar una serie de exigencias básicas, máxime cuando los órganos jurisdiccionales son parte de la maquinaria estatal y, por tanto, pueden mostrar cierto interés en salvaguardar las actuaciones de otros órganos del Estado, y de su propia policía judicial[47].

Esas ineludibles legislaciones deben preservar las garantías de las personas a la hora de evitar injerencias ilegales y discrecionales que vulnere algún derecho fundamental, pero principalmente, aquellas que atentan contra la intimidad. Evidentemente, se debe cumplir con los principios de necesidad[48] y proporcionalidad, siendo el gobierno el sujeto responsable de justificar la acción concreta por la cual se solicita la vulneración de esos derechos. Igualmente, junto a la no inversión de la carga de la prueba, esas leyes deben revestir el máximo nivel legislativo posible (en el caso español, deben investir la forma de Leyes Orgánicas), ser excesivamente precisas y concretas en las posibilidades

[46] D. RAYMAN LABRÍN, "Chile: Vigilancia y derecho", *cit*., pp. 189.

[47] Piénsese que estas labores de control social las realizan las Fuerzas y Cuerpos de Seguridad de un Estado, o los servicios de inteligencia, que serán los mismos que facilitarán o llevarán a cabo materialmente la instrucción de las causas penales, por lo que dichos excesos difícilmente se investigarán por parte de los operadores jurídico penales.

[48] Sólo puede vulnerarse la privacidad si no existe otra posible manera de perseguir un delito.

de intromisión y de la forma de proceder, para hacerlas lo menos lesivas con tales libertades esenciales, y así, proteger efectivamente ante el uso excesivo e ilegitimo, que podrían llevar a cabo los propios agentes que se encargan de la investigación[49].

Conjuntamente con mencionada propuesta, se debe acometer la protección de la libertad de expresión, de la intimidad y la privacidad, al menos, a través de los entes jurisdiccionales de tutela de los derechos humanos, tales como el Tribunal Europeo de Derechos Humanos y la Corte Interamericana de Derechos Humanos[50], toda vez que esa vigilancia sistemática y subrepticia, esa censura de las publicaciones por parte del Estado, es harto complicado de probar, por su propia naturaleza reservada y confidencial. Lógicamente, es necesaria dicha intervención de estas jurisdicciones internacionales, puesto que el Estado no querrá el castigo de sus propios agentes e instituciones, que permiten el mantenimiento del mismo, más aún si se tiene en consideración la situación de prevalencia del aparato estatal frente al ciudadano o grupos de ellos, individualmente considerados. Además, aún cuando se realice una vigilancia de la población a priori, para hacer valer las evidencias obtenidas de manera encubierta, se pueden utilizar autorizaciones judiciales al efecto de convalidar y refutar tal prueba ante los tribunales nacionales, que en este caso, no podrán sino tomar en cuenta y juzgar como legitima esa acreditación probatoria que se presenta al juicio, aún cuando genuinamente la misma se ha sustentado en una diáfana violación de los Derechos Humanos.

Finalmente, habría que advertir, que en todo caso, sería menesteroso incluir en los códigos penales de los Estados el delito relativo a la violación de la intimidad, llevada a cabo por medio de un control social y una vigilancia sistemática, bajo la argucia de mantener el orden social, en la que respondan por tales conductas antijurídicas los funcionarios públicos que desarrollan esas tareas de supervisión, igualmente sus superiores jerárquicos, e incluso, los propios políticos y autoridades estatales, en virtud del palmario conocimiento de estar cometiendo una violación de los derechos humanos y, aún así, continuar con dichas prácticas. Además, lógicamente, se hace indispensable utilizar junto con la pena en cuestión, una inhabilitación especial para ciertos cargos por tiempo determinado, como razonable consecuencia al tratarse de un delito especial ejecutado por miembros de la burocracia estatal. A mayor abundamiento, este mayor

[49] Informe del Consejo de Derechos Humanos de la Asamblea General de las Naciones Unidas *"El derecho a la Privacidad en la Era Digital",* publicado el 25 de marzo de 2015.

[50] Tutela no sólo contra los Estados totalitarios, sino respecto de los denominados democráticos.

reproche al que ejercita mencionada observancia represiva, no presentaría caracteres novedosos, puesto que se halla en la base de los delitos de lesa humanidad, crímenes de tortura o desapariciones forzadas, entre otros, puesto que éstos ostentan la singularidad de la persona del autor; la cual se halla en el seno de un dispositivo de poder (acaparando una posición aventajada, cuasi impune), atentando a sabiendas gravemente los derechos humanos de multitud de personas (afectación supraindividual), y requiriendo de cierta operatividad o una maquinaria organizada para poder llevar a cabo tales prácticas de supervisión y espionaje generalizado.

V. CONSIDERACIONES FINALES

Como corolario, simplemente sería reseñable manifestar que bajo ningún pretexto, los derechos o prerrogativas del Estado deben prevalecer sobre la protección de los derechos humanos, debido a que la institución denominada "Estado" es una invención propia del ser humano, y los derechos básicos de las personas no pueden quedar reprimidos por la omnipotencia de la maquinaria gubernativa estatal, ya que ello significaría despojar de los caracteres "humanos" a cada uno de nosotros.

Además, el control masivo de la ciudadanía en virtud de la salvaguarda de la seguridad, provoca una absoluta supresión de la seguridad jurídica, al eliminarse las garantías básicas con las que cuentan los individuos para desarrollarse en torno a su esfera moral de libertad. Por tanto, los beneficiados de la nimia regulación de la red, no son los particulares (que no pueden ejercer sus derechos fundamentales plenamente), sino por el contrario, son las grandes multinacionales y los gobiernos del mundo.

En este sentido, se debe mencionar imperiosamente que "*la seguridad nunca debe conseguirse a costa de la libertad de los ciudadanos, pues sin libertad nunca podremos estar seguros*[51]".

[51] A. E. PÉREZ LUÑO, "Internet y los derechos humanos", *cit.*, pp. 302.

VI. BIBLIOGRAFÍA

- H. BÉJAR, *El ámbito íntimo. Privacidad, individualismo y modernidad*, Alianza Editorial, Madrid, 1990.
- M. CASTELLS, *La era de la información: la sociedad red*, Alianza Editorial, 2ª Ed., Madrid, 2001.
- C. CASTILLA JUÁREZ, *Libertad de expresión y Derecho de Acceso a la Información en el Sistema Interamericano de Derechos Humanos*, Comisión Nacional de los Derechos Humanos, México, 2011.
- L. E. CÁZARES ROSALES, "Los derechos a la intimidad, a la propia imagen y al honor vulnerados por el ejercicio abusivo de la libertad de expresión en Facebook", en *Nueva Época*, núm 17, 2014.
- L. CORREDOIRA Y ALFONSO, "El derecho de acceso a la información en Internet", en *Actualidad Informática*, núm 32, 1999.
- A. ESTRADA CUZCANO, "Internet: cambio social, libertad e intimidad", *Escritura y Pensamiento*, núm 16, 2005.
- E. GARZÓN VALDÉS, "Optimismo y pesimismo en la democracia", en *Claves de Razón Práctica*, núm 131, 2003.
- G. GREENWALD, *Snowden. Sin un lugar donde esconderse*, Ediciones B, Barcelona, 2014.
- A. E. PÉREZ LUÑO, "Internet y los derechos humanos", *Anuario de Derechos Humanos, Nueva Época*, núm 12, 2011.
- M. RAGNEDDA, "Internet y control social. Entre Rizoma y Gran Hermano", en *Perspectivas de la Comunicación*, v. 4, núm 1, 2011.
- D. RAYMAN LABRÍN, "Chile: Vigilancia y derecho a la privacidad en Internet", en *Revista Chilena de Derecho y Tecnología*, v. 4, num 1, 2015.
- A. L. RUBIO MORAGA, "Censura en la red. Restricciones a la libertad de expresión en Internet", en VV.AA., *Prensa y periodismo especializado II,* Guadalajara, 2004.
- M. C. SABATER, "Vida de cristal. Análisis del derecho a la intimidad en la sociedad de la información", en *Intersticios. Revista Sociológica de Pensamiento Crítico*, núm 2, 2008.
- C. C. SUEIRO, "La criminalidad informática en el Anteproyecto de Código Penal de la Nación", *Revista Derecho Penal,* núm 7, 2014.
- VV.AA. "El control del ciberespacio por parte de gobiernos y empresas", en *Cuaderno Red de Cátedras Telefónica*, núm 9, 2012.
- R. WHITAKER, *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*, Paidós, Barcelona, 1999.