VIGILANCIA ELECTRÓNICA MASIVA, UNA INTROMISIÓN INDEBIDA DEL ESTADO: EL DERECHO INTERNACIONAL Y LA POSTURA ACTUAL DE LOS ESTADOS UNIDOS

ARTÍCULO

*Alexandra Cruz Zayas**

I. Introducción

"[*T*]*odas las personas deben ser tratadas con dignidad y respeto, independientemente de su nacionalidad o lugar de residencia y todas las personas tienen interés de privacidad legítimo en el control de su información personal."*[1]

El concepto privacidad tiene diferentes manifestaciones. Estamos acostumbrados a evitar divulgar algún asunto porque el mismo es parte o pertenece a nuestra vida privada pero, ¿qué significa la privacidad? Hablemos de al menos dos de sus manifestaciones. La privacidad es la falta de acceso de otra persona u otra entidad en lo que consideramos nuestra información personal. Existe, a su vez, la manifestación física de la privacidad. Esta se traslada a esa

---

* La autora es estudiante de segundo año y miembro del Cuerpo de Redactores de la Revista Jurídica de la Facultad de Derecho de la Universidad Interamericama de Puerto Rico.

[1] Cita del Presidente de los Estados Unidos de América, Barack Obama, durante un discurso en enero de 2014. Mark Stephens, *La Privacidad Después de Snowden, La Nación*, http://www.nacion.com/opinión/foros/privacidad-despues-Snowden_0_1424257573.html (accedido el 10 de noviembre de 2014).

morada que llamamos hogar la que defendemos de la intrusión de terceros. La privacidad como concepto ha evolucionado, no solo por el paso del tiempo sino por todos los adelantos tecnológicos, que de una forma u otra han modificado nuestro diario vivir. Información que solíamos solo escribir en papeles o transacciones oficiales ahora la depositamos en un mundo virtual por medio de una pantalla a través de un *click*.

No es un secreto que durante los últimos años la tecnología ha evolucionado. Es así como la tecnología se ha convertido en el eje central de las interacciones entre individuos. Esta misma tecnología es capaz de ser utilizada para una simple comunicación telefónica entre familiares, residentes en diferentes partes del mundo o como medio indispensable de comercio. Ante esta realidad, los usuarios de medios electrónicos se han visto en la necesidad de proveer información personal a diferentes entidades que proveen sus servicios de manera electrónica electrónicas para poder así gozar de los beneficios del internet. Esta información es suplida de manera no convencional. Estábamos acostumbrados a revelar números de cuenta, transferencias de dinero, llamadas de voz y comunicaciones escritas por medios convencionales como el papel, una visita al banco, el teléfono y hasta la carta. Sin embargo, algunos de estos medios parecerían estar obsoletos.

La Internet funciona de manera muy particular pues la información suministrada queda suspendida en un espacio cibernético no tangible.[2] Ello no le permite al individuo tener control absoluto de la información suministrada. No obstante, gracias a la información que los pasados meses se ha filtrado a través de los medios electrónicos, podemos concluir que cierta información que por necesidad se ofrece a una compañía electrónica parecería tener expectativa razonable de intimidad. Surge así la inquietud de cuánto abarca el derecho constitucional a la intimidad y el derecho al respeto de la vida privada del ser humano. La gran preocupación es quién tiene acceso a esa información suministrada a las redes electrónicas y cómo la utilizan.

La primera parte del trabajo pretende evaluar las posibilidades y el reconocimiento del derecho a la privacidad del individuo frente el derecho internacional y cómo algunos organismos internacionales han abarcado el problema y las propuestas que estos organismos han presentado. Esta primera parte se sub divide en dos. Comenzamos con el Consejo de los Derechos Humanos Naciones Unidas, del cual Estados Unidos es parte. El Consejo de los Derechos Humanos Naciones Unidas es un cuerpo que emite informes periódicos sobre las naciones estados y sus situaciones frente a los derechos humanos. Es de importancia mencionar la Convención de Monte Video la cual en sus primeros diez artículos nos define que se considera una nación estado o estado federal. Esta definición es importante pues el país debe cumplir con ella si pretenden participar o formar parte de algún pacto o comisión. Un estado federado es aquel que en su estructura máxima es capaz de representar

[2] *Id.*

todas sus unidades políticas.[3] Ante la consideración de esta definición tendríamos que concluir que Puerto Rico no es un estado federado capaz de representarse por sí mismo. Por lo tanto debido a nuestro estatus político Puerto Rico se ve representado por vía de los Estados Unidos. La segunda sub división es una mirada al otro lado del mundo mediante una de las Cortes con mayor influencia en la Unión Europea, la Corte Europea de Derechos Humanos. En la segunda parte de este escrito se hará una exposición de la situación y postura actual de los Estados Unidos. En la tercera parte abarcaremos el avance, si alguno de nuestra jurisprudencia ante ésta controversia. Culmino con alternativas ante la posibilidad de una controversia de índole cibernética frente a los tribunales de nuestro país. La idea es que al llegar una controversia que tenga como eje el derecho a la privacidad en los medios electrónicos se pueda utilizar este artículo como guía para posibles soluciones.

II. El derecho a la privacidad en el Derecho Internacional

El Derecho Internacional esta subdividido en dos vertientes: la privada y la pública. La diferencia entre ambas recae en el sujeto. Los abogados y profesores Barry Carter y Allen Weiner en su libro *International Law* definen estas vertientes como:

> Public International law was distinguished from private international law. Public international law primarily governed the activities of goverments in relation to other governments. Private international law deal with the entities when they crossed national borders.[4]

Durante este escrito discutiremos y analizaremos el ámbito público del derecho internacional. Para ello es de suma importancia identificar el sujeto a quien va dirigido el derecho internacional público: al estado nación.[5] Un estado nación, en su definición general es aquel capaz de firmar, negar o afirmar tratados con organizaciones fuera de su jurisdicción.[6]

El derecho internacional público comprende las normas de los derechos humanos. Ante el reconocimiento de los derechos humanos el derecho internacional busca proteger al individuo de acciones no favorables por parte del estado nación. El derecho internacional con un enfoque a los derechos humanos surgió luego de la Segunda

---

3 Montevideo Convention on the rights of the duties of States, art 1-10 (26 de diciembre de 1933). http://www.ilsa.org/jessup/jessup15/Montevideo%20Convention.pdf. (accedido el 14 de abril de 2015).

4 Barry Carter & Allen Weiner, *International Law*, 1-2 (Aspen Casebooks Series, Wolters Kluwer Law & Business, 2011).

5 Mario Daza & Karla Soto, *¿Cómo podemos definir el derecho internacional público?*, http://derechopublicomd.blogspot.com/2011/02/aspectos-generales-del-derecho.html (accedido el 4 de noviembre de 2014).

6 *Id.*

Guerra Mundial.[7] Sin embargo, las doctrinas originales de derecho internacional giraban en torno a los actos de una nación en contra de un extranjero.[8] Los derechos humanos a favor de un extranjero pueden reclamarse si la nación donde reside o visita el extranjero comete alguna falta en contra de este.[9] Es en estas circunstancias donde el estado nación del cual el extranjero es original actúa contra la nación que ha transgredido algún derecho humano. Esto se conoce como una protección diplomática.[10] Lo que quiere decir que como regla general el derecho internacional no es oponible a los estados naciones frente a una violación de algún derecho humano sobre sus nacionales.[11] Sin embargo, existen pactos entre naciones en los cuales se prometen a velar por los derechos, no solo de los extranjeros sino de sus propios nacionales.

Es muy común que los pactos internacionales se refieran al derecho a la privacidad como el derecho del ser humano al respeto a la vida privada.[12] El respeto a la vida privada es un concepto que se ha ido adoptando por los diferentes sistemas jurídicos constitucionalmente.[13] Esta tendencia de reconocer el derecho a la privacidad como un derecho de la más alta jerarquía para muchos países comenzó con la adopción de este derecho por organismos internacionales. La Declaración Universal de los Derechos Humanos adoptada el 10 de diciembre de 1948 por la Asamblea General de las Naciones Unidas constituyó una expresión de la comunidad internacional entorno a los derechos humanos. Estos principios fueron inspiración de muchas constituciones que le precedieron.[14] El artículo 12 de la Declaración Universal de Derechos Humanos dispone: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia . . ."[15]

Por otra parte, en 1948 se aprobó en Bogotá, Colombia la Declaración Americana de los Derechos y Deberes del Hombre. Esta Declaración dispone en su Artículo 5 del Capítulo 1 que: "[t]oda persona tiene derecho a la protección de la ley contra ataques abusivos a su honra, a su reputación y a su vida privada y familiar".[16] Con el mismo propósito se aprobaron tratados que reafirmaban la superioridad del derecho a la privacidad clasificándolo como uno de índole fundamental. Ejemplo de ellos lo

---

[7] *Id*.

[8] Sean Murphy, *Principles of International Law*, 293-338 (Concise Hornbook series, Thomson West 2006).

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id*.

[14] Jorge Carpio & Alonso Gómez, *El Derecho a la información y el respeto a la vida privada*, 97 Boletín Mexicano de Der. Comparado 23 (2000).

[15] Declaración Universal de los Derechos Humanos, art 12 (10 de diciembre de 1948), http://www.derechoshumanos.net/normativa/normas/1948-DeclaracionUniversal.htm (accedido 2 de noviembre de 2014).

[16] Declaración Americana de los Deberes y Derechos del Hombre, cap. 1, § 5 (2 de mayo de 1948), http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp (accedido 4 de noviembre de 2014).

son: la Convención Americana sobre los Derechos Humanos (1969),[17] el Pacto Internacional de Derechos Civiles y Políticos (1966),[18] A su vez la Convención Europea de Protección de los Derechos Humanos y Libertades Fundamentales (1950),[19] entre otros reafirman su compromiso a la protección de los derechos humanos.

La Convención Europea de Protección de los Derechos Humanos y Libertades Fundamentales es de gran importancia a la Unión Europea pues es pilar para las decisiones de la Corte Europea de Derechos Humanos.[20] Es por ello que la Corte ha interpretado extensamente el derecho de a la privacidad como: "actividades que permiten estrechar los vínculos de las personas con el mundo exterior".[21] Esta corte a su vez comenta que: "para que las injerencias de las autoridades públicas puedan ser lícitas deben estar previstas por ley, persiguiendo un fin legítimo . . ."[22]

A. El Consejo de los Derechos Humanos de las Naciones Unidas

El Consejo de los Derechos Humanos Naciones Unidas es un órgano intergubernamental que forma parte del sistema de Naciones Unidas y que se compone de 47 estados naciones.[23] Es meritorio recalcar que los Estados Unidos de América es miembro del Consejo de los Derechos Humanos de las Naciones Unidas como parte de las 47 naciones participantes. El propósito fundamental de este Consejo es velar por los derechos humanos. Para lograr su propósito formulan recomendaciones que son publicadas para que las naciones tomen conocimiento de las violaciones de los derechos humanos y puedan cesar o disminuir las mismas.[24]

El 17 de abril de 2013, el Consejo de Derechos Humanos Naciones Unidas emitió un informe que abordó el derecho a la privacidad en las redes electrónicas.[25] En las primeras páginas se demarca la preocupación entorno a la intromisión de los estados naciones en la vida íntima de los individuos.

El derecho a la privacidad es reconocido por organismos internacionales y aunque se conoce de su existencia no sabemos a ciencia cierta hasta donde llega su protec-

---

[17] Convención Americana sobre los Derechos Humanos, cap. 2, art. 11 (22 de noviembre de 1969), http://www.oas.org/dil/esp/tratados_B-32_Convencion Americana_sobre _Derechos_Humanos.htm. (accedido 4 de noviembre del 2014).

[18] Pacto Internacional de Derechos Civiles y Políticos. parte. 3, art. 17 (16 de diciembre de 1966), http://www.derechos.org/nizkor/ley/pdcp.html. (accedido 4 de noviembre de 2014).

[19] Convenio Europeo de Protección de los Derechos Humanos y Libertades Fundamentales, título. 1, art. 8 (4 de noviembre de 1950), http://www.echr.coe. int/Documents/ Convention_SPA.pdf. (accedido 2 de noviembre de 2014).

[20] *Id.*

[21] Jorge Carpizo & Alonso Gómez, *supra* n. 4, pág. 35.

[22] *Id.*

[23] Naciones Unidas Derechos Humanos, *Consejo de Derecho Humanos*, http:// www. Ohchr .org/SP/HRBodies/HRC/Pages/AboutCouncil.aspx (accedido el 4 de noviembre de 2014).

[24] *Id.*

[25] *Report of the Special Rapporteur on the promotion and protection and protection of the right to freedom of opinion and expression*, UN GE, 23 Sess., Supp. No.3, UN Doc. A/16/4 (2013).

ción.. Es por ello que es difícil delimitar su aplicabilidad. En el Informe Especial del Consejo de las Naciones Unidas, [en adelante Informe Especial] se define privacidad como un área de auto desarrollo e interacción personal lo que crea una esfera privada.[26] La privacidad se reduce a la habilidad del individuo de contener información sobre sí y cómo esa información es utilizada.[27]

El Informe Especial propone que se evalúen las restricciones permisibles al derecho a la privacidad mediante seis elementos: 1) cualquier restricción debe ser provista por ley; 2) la esencia del derecho humano no puede ser sujeto de restricciones; 3) las restricciones son necesarias en una sociedad democrática; 4) cualquier ejercicio de discreción en la aplicación de la restricción no deber ser ilimitada; 5) para que una restricción sea permisible no es suficiente que sirva uno de los objetivos enumerados. La misma debe ser necesaria para alcanzar un objetivo legítimo; y 6) las medidas restrictivas deben ajustarse al principio de proporcionalidad, deben ser apropiadas para lograr su función de protección, deben ser el instrumento menos perturbador de los que permiten conseguir el resultado deseado y deben guardar proporción con el interés que debe proteger.[28]

La propuesta de estos postulados para la protección de la privacidad del individuo surge ante las justificaciones gubernamentales sobre el uso de la vigilancia para combatir el terrorismo. Con esta excusa los gobiernos se han manejado para obtener no solo información confidencial (textos, números de teléfonos, correos electrónicos etc.) sino también contraseñas y nombres de usuarios en las redes sociales. Muchos gobiernos logran obtener esta información mediante pedidos de comunicaciones que le hacen a compañías privadas como por ejemplo: Google. Google ha reportado que el número de pedidos por parte del gobierno se ha duplicado del 12,539 en los últimos seis meses del 2009 a 21,389 en los últimos seis meses de 2012.[29] Es por ello que el Consejo de las Naciones Unidas busca la implementación de los seis elementos propuestos para evaluar principios de proporcionalidad.[30] La proporcionalidad se atañe a los estándares internacionales de derechos humanos y les exige a los gobiernos justificar las medidas que tomen a base de la necesidad de las mismas y la evaluación de métodos que se han utilizado para la protección del individuo ante la posibilidad del abuso.[31] Esta propuesta intenta evitar la violación de un derecho humano por un gobierno mediante la intrusión masiva.

El Informe Especial concluye con unas recomendaciones adheridas a estándares legales. Menciona que la vigilancia de las comunicaciones solo debe ocurrir por las circunstancias más excepcionales y exclusivamente bajo la supervisión de una au-

---

[26] *Id*. pág. 6.
[27] *Id.*
[28] *Id*. págs. 8-9.
[29] Alberto Escudero & Gus Hosein, *Questioning Lawful Access to Traffic data*, Communications of the ACM, vol. 47, 77-82 (2004).
[30] *Id.*
[31] *Report of the Special Rapporteur on the promotion and protection and protection of the right to freedom of opinion and expression*, *supra* n. 11, pág. 9.

toridad judicial independiente.[32] Expresa que el individuo debe ser notificado que es sujeto de vigilancia y que esa información obtenida está siendo utilizada por el estado.[33]

B. La Corte Europea de Derechos Humanos

La Corte Europea de Derechos Humanos, (en adelante la Corte Europea) se estableció en 1959 y como producto de ello surge el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales.[34] Para que un Estado pueda ser denunciante o denunciado tiene que haber ratificado la Convención Europea de Derechos Humanos. La Corte Europea de los Derechos Humanos procura proteger los derechos garantizados en el Tratado Internacional de los Derechos Humanos que es parte de la Convención Europea. El artículo 8 del Tratado de la Convención Europea reconoce la privacidad y declara:

> Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho salvo cuando esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de terceros.[35]

A diferencia del Consejo de las Naciones Unidas la Corte Europea de Derechos Humanos tiene la capacidad de ordenarle al estado que tome las medidas provisionales para proteger los derechos individuales de forma transitoria en lo que se termina de evaluar el pleito.[36] La Corte Europea refiere casos a la Gran Cámara cuando es necesario una interpretación compleja de los derechos humanos.[37] La sentencia de la Gran Cámara es final y firme. Estas sentencias logran poner presión política y económica al Estado. Incluso la Corte Europea de Derechos Humanos y cualquiera de sus divisiones tiene el poder de enviar casos nuevamente a sus Cortes si un país ha fallado en implementar las sentencias.[38]

---

[32] *Id.*

[33] *Id*. pág. 21.

[34] La Red Global: Defendiendo y Promoviendo la Libertad de Expresión*, Corte Europea de Derechos Humanos,* http://www.ifex.org/campaigns/european_court_human_rights/es/ (accedido el 4 de noviembre de 2014).

[35] Convención Europea de Derechos Humanos, art. 8 (3 de septiembre de 1953), http:// www.acnur.org/t3/fileadmin/scripts/doc.php?file=biblioteca/pdf/1249 (accedido 2 de noviembre de 2014).

[36] La Red Global: Defendiendo y Promoviendo la Libertad de Expresión, *supra* n. 34.

[37] *Id*.

[38] *Id.*

La Gran Cámara emitió el pasado 13 de mayo de 2014 una sentencia en el caso *Google v. Agencia Española de Protección de Datos* (en adelante A.E.P.D.).[39] La controversia de este caso giraba en torno al procesamiento de información personal y el libre movimiento de esta información. La A.E.P.D. argumentaba que la Gran Cámara debía ordenarle a Google la adopción de medidas necesarias para detener la recolección de información de un individuo específico y prevenirlos de obtener información en el futuro. La Corte utiliza el artículo 8 del Tratado Internacional de la Convención Europea de los Derechos Humanos[40] como parte de su análisis que culmina en la implementación de la directiva 95/46 como parte de su resolución. Las directivas son el corolario de lo que en los tribunales locales llamaríamos opiniones. Se les llama directivas pues no tienen fuerza extrínseca de ley y son una especie de guías para las naciones. Esta directiva puntualizaba sobre la protección de los derechos fundamentales como lo es la libertad, en particular su derecho a la privacidad.[41] La directiva crea la posibilidad de procesar la información personal con respeto asegurando un alto nivel de protección.[42]

La directiva 95/46 es parte de los postulados relacionados con la calidad de la información. En apoyo a esta directiva y sus postulados la Corte Europea de los Derechos Humanos utiliza como método persuasivo el capítulo 2 en su artículo 6 que establece lo siguiente:

> Member States shall provide that personal data must be:
>
> (a) Processed fairly and lawfully;
>
> (b) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
>
> (c) Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
>
> (d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
>
> (e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
>
> It shall be for the controller to ensure that paragraph 1 is complied with.[43]

---

[39] *Case concerning the personal data* (Google v. AEPD), 2014 E.C.H.R.

[40] Convención Europea de Derechos Humanos, *supra* n. 18.

[41] *Id.*

[42] *Case concerning the personal data, supra* n. 21, pág. 12.

[43] *Principles Relating to Data Quality*, cap. 2, art. 6 (24 de octubre de 1995), https:// www. cdt.org/files/privacy/eudirective/EU_Directive_.html#HD_NM_6. (accedido 30 de octubre de 2014).

Concluye la Corte Europea de los Derechos Humanos que al utilizar la directiva 95/46 y los Principios Relacionados con la Calidad de la Información evita que se utilice la información para cualquier otro propósito que no fuese por lo que fue sustraída en un principio. La directriz y el reconocimiento de principios relacionados con la calidad información le permiten a aquellas naciones estados que se someten voluntariamente a la jurisdicción de la Corte Europea de los Derechos Humanos la posibilidad de unos postulados uniformes. Esta uniformidad permitirá atender controversias de manera más objetiva.

III. La privacidad en las redes electrónicas en los Estados Unidos

Si bien es cierto que el derecho a la privacidad no está explícitamente consagrado en la Constitución de los Estados Unidos de América, nadie puede dudar de su existencia. La jurisprudencia le ha dado vida a este derecho en casos como *Roe v. Wade*.[44] En este caso el Tribunal Supremo de los Estados Unidos reconoce la existencia del derecho a la vida privada e íntima bajo la Enmienda 14 de la Constitución de los Estados Unidos.[45] Al igual que este caso la jurisprudencia sigue reconociendo el derecho a la privacidad e intimidad como aquel que emana de las "penumbras" de la Constitución.[46] Sin embargo, parece ser que definir los límites de la protección constitucional en el mundo virtual es una controversia difícil de resolver.[47]

Uno de los casos más emblemáticos resueltos por el Tribunal Supremo de Estados Unidos lo es *Smith v. Maryland*[48] en el cual el Juez Blackmun escribe la opinión de la mayoría y hace la distinción de la información de contenido y la información de no contenido. En este caso se discute la posible obtención de información por medios electrónicos sin orden judicial *vis a vis* la protección de la Cuarta Enmienda de la Constitución de los Estados Unidos. Los hechos de este caso giraban en torno a la expectativa de intimidad que posee el individuo sobre los números llamados desde su teléfono. El Tribunal decide que por el solo hecho de marcar los números el individuo estaba renunciando a su expectativa de intimidad pues sabía que los mismos estaban automáticamente a la disposición de la compañía telefónica.[49] Por lo tanto, el individuo, según la opinión mayoritaria, renunció a su expectativa de intimidad al momento en que realizo la llamada. En esta doctrina el Tribunal Supremo hace la salvedad de que los números llamados no se clasifican como información de contenido porque de serlo estarían protegidos por la Constitución. La Cuarta Enmienda de la Constitución de los Estados Unidos es analizada nuevamente por el Tribunal Su-

---

[44] *Roe v. Wade*, 410 U.S. 113 (1973).

[45] Cont. EE.UU. enm. XIV, § 1.

[46] *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965).

[47] Camille Álvarez, *Desvanece la intimidad en el mundo virtual: La Búsqueda de Protección Constitucional en Internet*, 45 Rev. Jurídica U. Inter. P.R., 265, 267 (2011).

[48] *Smith v. Maryland*, 422 U.S. 735 (1979).

[49] *Id.*

premo de los Estados Unidos en una situación de hechos similares. El Tribunal optó por adoptar la teoría de asunción de riesgo.[50] Esta teoría se basa en que el individuo asume el riesgo de que su información termine en manos del gobierno al cederla a terceros. Estos terceros tendrían el poder de disponer de la información que con anterioridad le fue ofrecida.

La administración del Presidente Barack Obama se enfrentó el 5 de junio del 2013, con este panorama jurisprudencial deferente a la obtención de información por parte del gobierno. Ese día ocurrió el escándalo de filtraciones de información clasificada más grande de la historia. El periódico Británico *The Guardian* reporta múltiples informes que resultaban ser información clasificada del gobierno de los Estados Unidos por parte de un empleado de la Agencia de Seguridad Nacional estadounidense (en adelante N.S.A.), Edward Snowden.[51] Entre los documentos filtrados se encontraba la corroboración sobre la existencia de programas de vigilancia masiva a civiles. Uno de ellos lleva por nombre PRISM.[52] Este programa le permite al gobierno acceder a los servidores de algunas de las principales compañías tecnológicas como lo son Google, Yahoo, Microsoft, etc.[53] De igual forma salió a la luz información pública sobre la existencia de muchísimos programas de vigilancia masiva. Programas como PRISM le permite al gobierno obtener conversaciones telefónicas, *metadata* y hasta la posibilidad de armar un perfil completo del individuo.[54]

La noticia sobre la existencia de programas que le permitían al gobierno recopilar un sin número de información personal contenida en las redes electrónicas desato el descontento de los usuarios. Su descontento se comenzó a notar mediante las quejas a sus proveedores, compañías de redes electrónicas. Las compañías por su parte comienzan acciones legales contra los Estados Unidos por no permitirles brindar información a sus consumidores de la cantidad de pedidos por parte del gobierno.[55] El propósito de esto era informar a sus clientes sobre la obligación que tenían de proveer la información del individuo para con el gobierno. Para hacer escuchar sus reclamaciones las partes tienen que acudir a un foro especial. Este foro lleva por nombre el *United States Foreing Intelligence Surveillance Court* (en adelante F.I.S.C.). La F.S.I.C. fue establecida en el 1978 mediante la aprobación del *Foreing Intelligence Survillance Act*.[56] La Corte tiene como cede Washington D.C y está compuesta por jueces de los Tribunales de Distrito que han pasado un proceso de *clearance* y sirven

---

[50] *Unites States v. Miller*, 425 U.S. 435 (1976).

[51] *Klayman v. Obama*, 957 F. Supp.2d 1, 10 (2013).

[52] José Méndez, *Espionaje en Estados Unidos: Seguridad v. Privacidad*, Unocero, http:// www.unocero.com/2013/06/20/espionaje-en-estados-unidos-seguridad-vs-privacidad/ (accedido el 4 de noviembre de 2014).

[53] *Id.*

[54] *Id*.

[55] *Id*.

[56] Foreign Intelligence Surveillance Court, *About the Foreign Intelligence Surveillance Court*, http:// www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (accedido el 4 de noviembre de 2014).

por ciclos de siete días.[57] Debido a que los jueces solo tienen acceso a las peticiones por siete días la Corte tiene un comité de trabajo compuesto por investigadores y abogados que se dedican a entrevistar testigos y recopilar información necesaria para completar las alegaciones o mociones.[58] Estas mociones pueden ser llevadas a la atención de la Corte por el Gobierno para buscar alguna aprobación, comenzar una vigilancia electrónica o por alguna organización no gubernamental que debe acatar alguna orden del gobierno.[59] Estas órdenes o directivas gubernamentales tienen que ir dirigidas a temas de vigilancia electrónica, o a archivos de negocios, colección de la *metadata* y la desclasificación de alguna información clasificada por el Director de Inteligencia Nacional.[60] Las decisiones de esta Corte pueden ser apeladas bajo la F.I.S.C.A. que es la división apelativa de la F.I.S.C. Si después de la decisión de la F.I.S.C.A. una de las partes aún desea apelar solo queda el recurso de *certiorari* al Tribunal Supremo de los Estados Unidos.[61]

Es mediante la F.I.S.C. que las plataformas electrónicas como Yahoo deciden presentar una moción para que se les permita notificar a sus clientes si han sido objeto de vigilancia.[62] Para la compañía Yahoo era importante desligarse de las violaciones denuncias por las filtraciones de documentos en el 2013.[63] La única forma de lograrlo era presentando una moción a la F.I.S.C. para que mediante una orden judicial se le ordenara al gobierno de los Estados Unidos desclasificara las ordenes de vigilancia electrónica y le permitiera a la compañía Yahoo publicarlas. Esto para que pudiera al menos dar a conocer la cantidad de información que el gobierno obtenía mediante su red. Yahoo hace la aclaración que en los reportes de transparencia que pretende emitir no se incluirá información de individuos particulares relacionados con las peticiones gubernamentales como parte de sus investigaciones para la protección de seguridad nacional.[64] La inhabilidad de no poder publicar los informes de transparencia con los números de la cantidad de personas que son investigadas, tiene como consecuencia un daño a la reputación de la compañía e incertidumbre en sus negocios no solo en Estados Unidos sino a nivel mundial.[65] La compañía utiliza como argumento Constitucional su derecho a publicar cobijado en la Primera Enmienda de la Constitución de los Estados Unidos. El riesgo a la seguridad nacional de publicar la cantidad de

---

[57] Ltr. From Hon. Reggie Waltin, Pres., U.S. States Foreign Intelligence Surveillance Court, to Hon. Patrick Leahy, Chairman, Committee on the Judiciary, Response Letter, 4 (29 de julio de 2013) http://www.fisc. uscourts.gov/ sites/default/files/ Correspondence%20Leahy-1.pdf (accedido 4 de noviembre de 2014).

[58] *Id*. pág. 6.

[59] *Id.* pág. 2.

[60] *Id*. pág. 1.

[61] *Klayman*, 957 F. Supp. 2d pág. 14.

[62] Yahoo!'s Mot. For Declaratory Judgment to disclose aggregate data, *Yahoo!'s v. U.S.* (States Foreign Intelligence Surveillance Ct., 2013) (No. 13-05).

[63] *Id.*

[64] *Id*.

[65] *Id.* pág. 3.

personas o la cantidad de órdenes que se han recibido por parte del gobierno es minúsculo pues no importa el número revelado la compañía la inmensidad sus de usuarios hace prácticamente imposible que alguno de ellos pueda identificarse.[66] La prohibición del gobierno a estas publicaciones sería una restricción de palabra basada en contenido lo que es sujeto a un escrutinio estricto.[67] Para sobrevivir este escrutinio el Gobierno tendría que presentar y defender un interés apremiante. El Tribunal Supremo de los Estados Unidos ha concluido en *Mitchell v. Forsyth*[68] que las determinaciones de oficiales de la rama ejecutiva del país fundadas mediante el pretexto de la seguridad nacional no tienen inmunidad absoluta. Yahoo concluye en su moción que no hay razón para seguir denegando la publicación de la cantidad de órdenes que reciben para la vigilancia por parte del gobierno pues el propio Presidente Barack Obama en su discurso luego de las filtraciones del 2013 le pidió al Director de la Agencia de Inteligencia Nacional que desclasificara la mayor información posible sobre programas de vigilancia masiva.[69]

Las demandas y causas de acción en contra del gobierno por razón de las violaciones de los derechos humanos por sus programas de vigilancia masiva llego a las cortes civiles. Larry Klayman, un abogado y activista de los derechos humanos quien es usuario y cliente de la compañía telefónica Verizon, llega a la Corte de Distrito de Washington D.C reclamando una violación por parte del gobierno de las Enmiendas I, IV y V de la Constitución de los Estados Unidos.[70]

El caso comienza con la descripción de la sección 215 del *Patriot Act*[71] la que faculta al Gobierno de los Estados Unidos a hacer búsquedas tangibles. El concepto de búsqueda tangible lo define la ley como: "for an order requiring the production of any tangible things (including books, records, paper documents, and other items) for an investigation to obtain foreign intelligence."[72] Sin embargo, a esta ley el Congreso le hizo una enmienda en el 2006, en la sección 1861 del *Patriot Act*, se añade que debe existir motivo razonable para la búsqueda de material tangible y hacer de ella material de investigación.[73] Estos procedimientos tienen que ir acorde y deben ser aprobados por la F.I.S.C. El resultado de esta enmienda fue la recolección masiva por parte del FBI, quienes almacenaban la información extraída directamente de las compañías de telecomunicaciones.[74] El almacenamiento de la información que recopilaban las agencias de inteligencia a diario les permitía hacer un análisis retrospectivo.[75] Al resolver el caso la F.I.S.C. mencionó que esta información almacenada solo podría

---

[66] *Id.*

[67] *Id*. pág. 6. (citando a *Doe v. Mekasey*, 549 F. 3d 861, 878 (2d Cir. 2008).

[68] *Mitchell v. Forsyth*, 472 U.S. 511 (1985).

[69] Yahoo!'s Mot. For Declaratory Judgment to disclose aggregate data, *supra* n. 62, pág. 8.

[70] *Klayman,* pág. 10.

[71] Pub. L. No. 107-56, 215, 115 Stat. 272 (2001).

[72] *Id*.

[73] *Klayman,* pág. 11.

[74] *Id.*

[75] *Id.*

asesarse para contrarrestar acciones terroristas. Sin embargo la información filtrada por Snowden en el 2013 demostró que la N.S.A. analizaba retrospectivamente la información sin aprobación judicial o un *reasonable articulate suspicion*.[76] Accesaban los números de teléfonos que tenían en sus bases de datos y los utilizaban como "hop"[77]. Repetían esta operación hasta tres veces con cada número que obtenían del inicial.[78]

La F.I.S.C. se ha caracterizado por manejar mociones y controversias *ex parte* de manera secreta lo que resulta en opiniones de materia clasificada. Este es el caso de la controversia surgida en *Klayman v. Obama.* En este casi se discute si una tercera parte civil podía llevar la causa de acción contra la N.S.A. y si la corte de Distrito tiene jurisdicción. La Corte discute que la ley que crea el F.I.S.C., el *Foreign Intelligence Surveillance Act*,[79] no incluye un derecho de revisión judicial expreso para con un tercero por lo que la Corte no está prohibida de atender un asunto constitucional relacionado con los postulados que la F.I.S.C. resuelve.[80] Teniendo el asunto de la jurisdicción resuelto, el Tribunal de Distrito pasa a considerar los asuntos constitucionales. El demandante argumenta que la mera colección de información sin motivo justifica una violación a la Cuarta Enmienda de la Constitución de los Estados Unidos. Por otra parte, el Estado utiliza el precedente de *Smith v. Maryland*[81] donde el gobierno argumenta que se utilizó la tecnología llamada *pen register*. Esta tecnología logra captar los números de teléfonos en llamadas entrantes de una unidad en particular.[82] Esta decisión del Tribunal Supremo sí resulto constitucional pero el Tribunal de Distrito la diferencia mediante dos argumentos: 1. que sin duda la tecnología ha avanzado y al interferir un celular se puede obtener mucho más que los números de las llamadas entrantes o salientes; y 2. que en este caso el dispositivo estaba configurado para intervenir una unidad específica. Cita el Tribunal a *Mills v. District of Columbia* y menciona que: "It has been establish that the loss of the constitutional freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury."[83] Como tal las lesiones irreparables del derecho constitucional frente a un interés del estado deben someterse a un análisis cuidadoso ante un balance de interés.[84] Por lo que concluye que esta recolección de información sí da paso a una violación Constitucional pero de la misma forma reconoce que la interpretación de esta controversia es de gran complejidad por lo que el Juez Richard de León culmina

---

[76] *Id.* pág. 12.

77 Un "hop" es el nombre de una técnica. Este modo de recolección de datos se define como la obtención de un número madre y con este se obtenían todos los números a quienes se llamaban desde el número inicial. Ello cree la posibilidad de una cadena de obtención de datos interminable.

[78] *Klayman,* pág. 17.

[79] 50 U.S.C § 1801-1871 (1978).

[80] *Klayman*, 957 F. Supp. pág. 17.

[81] *Smith v. Maryland*, 422 U.S. 735 (1979).

[82] *Klayman*, 957 F. Supp. pág. 20.

[83] *Mills v. District Of Columbia*, 571 F. 3d 1304, 1312 (2009).

[84] *Klayman*, 957 F. Supp. pág. 26.

su memorando de opinión dejando la controversia pendiente para un proceso apelativo.[85] Parece ser que este caso tiene posibilidades de llegar a la Corte Suprema de los Estados Unidos. Ello con la posibilidad de que el Tribunal Supremo de los Estados Unidos se exprese y delimite lo abarcador que pueden ser las protecciones Constitucionales en el internet y como el Estado debe adherirse a las mismas.

IV. Puerto Rico y su protección Constitucional en las plataformas electrónicas

A diferencia de la Constitución de los Estados Unidos, nuestra Constitución es expresa cuando menciona que la dignidad del ser humano[86] es inviolable y protege al individuo ante ataques a su honra, su reputación, su vida privada y familiar.[87] Es así como el Tribunal Supremo de Puerto Rico a través de la jurisprudencia ha interpretado los derechos concebidos en nuestra Constitución como unos de factura más ancha.[88] En *Figueroa Ferrer v. ELA* el Tribunal nos dice: "[e]n ausencia de intereses públicos apremiantes el Estado no puede violar la zona de intimidad protegida por el Art. II, Sec. 8 de nuestra Constitución."[89]

Los Tribunales del país no se han enfrentado a una controversia que acarree los límites de la protección Constitucional en el internet. Sin embargo tenemos opiniones de nuestro más alto foro que deciden sobre temas Constitucionales en la utilización de medios electrónicos. Un ejemplo de ello lo es el caso de *P.R.T.C. v. Martínez*.[90] Este caso es una excepción a la norma pues en Puerto Rico existe una prohibición Constitucional a la intercepción de llamadas telefónicas, sin embargo, se permite la intercepción pues la misma contaba con el consentimiento de la mujer que había recibido las llamadas hostigantes.[91] Recordemos que no existe en Puerto Rico tal cosa como un derecho absoluto por lo que aún la intimidad y la vida privada tiene sus límites o en este caso excepciones. Un caso más reciente lo es *Rosario v. Wapa*.[92] A pesar de que es un caso del Tribunal Apelativo, el tribunal evalúa el derecho Constitucional a la intimidad y la vida privada de una pareja homosexual en contra prestación a la libertad de prensa de un programa televisivo. En este caso una pareja homosexual pretendía celebrar su relación en una ceremonia íntima que procuraron mantener lo más privada posible para evitar una reacción pública, mientras que el canal televisivo demandado llevo cámaras y reportó la ceremonia en *prime time* logrando un desborde de opiniones públicas diversas. Para rebatir el argumento de expectativa de intimidad de la pareja, Wapa utiliza una invitación electrónica que

---

[85] El proceso apelativo de este caso está en proceso a la fecha de la redacción de este artículo.
[86] Const. P.R. Art. II, § 1.
[87] Const. P.R. Art. II, § 8.
[88] *Figueroa Ferrer v. ELA*, 107 D.P.R. 250, 258 (1978).
[89] *Id.* pág. 275.
[90] *P.R.T.C. v. Martínez*, 114 D.P.R. 328, 359 (1983).
[91] Const. P.R. Art II, §10.
[92] *Rosario v. Wapa Tv, Inc.*, sentencia de 29 de agosto de 2014, KLAN 201400120.

le hiciera la pareja a Ricky Martin por la red social Twitter. Alegando así que la pareja sí divulgo el evento convirtiéndose en un tema de interés general. El Tribunal falló a favor de la pareja pero no entró en detalles sobre la utilización de las redes sociales y sí en realidad estaban renunciando a su expectativa de intimidad por la publicación del evento. La Corte incluso menciona que el Estado no presentó prueba de que ésta publicación en la red social fuera una accesible a todo el que formara parte de ella o que cualquiera pudiera acceder a ver la invitación. El Tribunal deniega la sentencia sumaria que presentó el demandado y aclara que no se presentó prueba inequívoca de que las acciones de los demandados dieran paso a una renuncia clara de su derecho a la intimidad y la vida privada enviando el caos nuevamente al Tribunal de Primera Instancias para un descubrimiento de prueba.

La legislación puertorriqueña atiende el tema del espionaje cibernético desde el aspecto puramente comercial. La Reglamentación de Negocios de la *Ley de Regulación de Espionaje Cibernético*[93] define *Spyware* o programa de espionaje cibernético como: "Cualquier programa que corra o ejecute funciones en una computadora sin el consentimiento informado del dueño o usuario autorizado de la computadora." Mientras que en su sección 2185 prohíbe: "el uso o instalación de Spyware en una computadora, para cualquier propósito, a no ser que medie el consentimiento informado y expreso del dueño o usuario autorizado de ésta".[94] A pesar que para el año 2010 la Cámara de Representantes aprobó por unanimidad la creación de un *Cyber Code* no paso a ser mucho más que eso. El proyecto no llegó a ser ley. El *Cyber Code* intentaba proteger el derecho a la intimidad del individuo en las redes electrónicas pero abarcando el ámbito penal.[95] El proyecto carecía de apoyo de los medios de comunicación y de empatía general.[96] Por todo lo anteriormente discutido podemos concluir que Puerto Rico no ha atendido la controversia de las protecciones Constitucionales en las plataformas electrónicas.

V. Conclusiones y recomendaciones

El derecho a la intimidad y la vida íntima parecerían ser pilares fundamentales en nuestro sistema de derecho. Sin embargo, existen aún áreas muy grises donde no podemos delimitar hasta donde llega su alcance. El uso de las redes electrónicas como la Internet, está en aumento y debemos estar preparados. La preparación debe comenzar con una actualización a nuestro sistema legal. Es idóneo que nuestra Asamblea Legislativa retome el proyecto del *Cyber Code* pero con una visión distinta. Dirigir este proyecto hacia la protección de los derechos humanos. Así cada individuo podrá estar seguro hasta donde está protegido y decidir que debe y puede compartir en sis-

---

[93] *Ley de Regulación de Programación de Espionaje Cibernético*, Ley Núm. 165-2008, 10 L.P.R.A. § 2181 (Lexis 2013).

[94] *Id*. § 2183.

[95] Álvarez, *supra* n. 28, pág. 281.

[96] *Id.*

temas electrónicos como el internet. El caso civil *Klayman v. Obama*[97] a la fecha está siendo considerado por el tribunal de distrito de apelaciones de Washington D.C. Debido a lo novel de la controversia es muy posible que este caso civil llegue al Tribunal Supremo de los Estados Unidos. Mientras tanto nos parece que es necesario tomar y adoptar la doctrina propuesta por los dos organismos internacionales discutidos con anterioridad quienes parecen ambos sugerir un escrutinio estricto. El escrutinio estricto es sugerido cuando se ve envuelto el gobierno por sus actos de vigilancia *vis a vis* la invasión de la vida privada e íntima del individuo. Ante la existencia de parámetros legales, esfuerzos legislativos, y la interpretación bajo un escrutinio estricto, el individuo podrá asegurarse que aquello que se obtenga y se utilice en su contra cede ante un interés apremiante del estado y no se recolecta información por mero capricho. Es momento de que las autoridades legislativas den un paso adelante ante el mundo de posibilidades que es la Internet y evite la violación masiva de derechos humanos. Espero que este trabajo sirva como propuesta ante la existencia de un mundo no tangible capaz de violar la dignidad del ser humano. Con esperanzas de que este trabajo sirva de guía a la legislatura tanto como a los tribunales cuando surja ante sí la controversia cito al Juez Marshall:

> [I] do not believe that the meaning of the Constitution was forever "fixed" at the Philadelphia Convention. Nor do I find the wisdom, foresight, and sense of justice exhibited by the Framers particularly profound. To the country, the government they devised was defective from the start, requiring several amendments, a civil war, and momentous social transformation to attain the system of constitutional government, and its respect for the individual freedoms and human rights, we hold as fundamental today. When contemporary Americans cite "The Constitution" they invoke a contempt that is vastly different from what the Farmers barely began to construct two centuries ago . . .[98]

Ante estas expresiones resulta beneficioso y bastante evidente que debemos recurrir a las variaciones y doctrinas del derecho internacional público. Ello debido a que las mismas se han desarrollado con mayor rapidez. A pesar de que el derecho internacional público no resulte vinculante sin duda es material de análisis pues su redacción va dirigida a la protección de los derechos humanos frente a las naciones estados, provee así una demarcación más amplia y clara de las posibles protecciones constitucionales.

---

[97] *Klayman*, 957 F. Supp. 2d. pág. 1.

[98] Raúl Serrano, *Derecho Constitucional de Estados Unidos y Puerto Rico* tomo II, vol. II, 1021 (4ta ed., Universidad Interamericana de Puerto Rico, Facultad de Derecho 2013) (citando Marshall, *Justice Marshall Speaks*, The Center for Constitucional Rights Looks at the Constitution, 9-11 (1987).