DESVANECE LA INTIMIDAD EN EL MUNDO VIRTUAL: LA BÚSQUEDA DE PROTECCIÓN CONSTITUCIONAL EN INTERNET

ARTÍCULO

*Camille Álvarez Jacobo**

I. Introducción

> There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, [they] plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time . . . . You had to live . . . in the assumption that every sound you made was overheard, and . . . every movement scrutinized.[1]

Imaginemos un mundo donde, al mudarnos a una casa, el Gobierno exija que se le permita instalar cámaras de video en cada habitación; que para instalar una línea telefónica en la casa, haya que darle autorización a la compañía

* La autora es egresada de la Facultad de Derecho de la Universidad Interamericana de Puerto Rico. Fue miembro del Cuerpo de Redactores de la Revista Jurídica y, durante su tercer año, fue Directora Asociada de la Revista Jurídica. La autora desea agradecer al Profesor Carlos Ramos González por su orientación en el tema durante las etapas preliminares del desarrollo de este Artículo.

[1] George Orwell, *Nineteen Eighty-Four* 3 (100ma ed., Penguin 2003).

telefónica para que grabe todas las conversaciones telefónicas; que para poder recibir correspondencia, se le permita al cartero leer la correspondencia y fotocopiar aquellas cartas que le interesen; que para acceder los fondos de una cuenta, se le permita al banco mantener un registro de todas las transacciones y que para salir de la casa, se le ponga un grillete electrónico a cada persona para que rastree cada uno de sus movimientos.

La idea de un mundo donde nuestros asuntos más íntimos estén bajo el escrutinio de terceros o incluso del Gobierno parece absurda y, más aún, ilegal. Pero para los que utilizamos el Internet a diario, ya sea para comunicarnos, efectuar transacciones bancarias, comprar o simplemente navegar, el supuesto anterior se convierte en una cruda y triste realidad.

Aunque hay cierta protección constitucional a la intimidad en el Internet, su límite y su alcance aún no han sido definidos con exactitud. Surge la interrogante de si debe el Gobierno tener acceso a la estela de información que trazamos en Internet. De ser así, surge además la duda de ante qué supuestos una compañía privada le puede dar información al Gobierno. Por estar el derecho a la intimidad en juego, ¿se requiere un estándar más riguroso para exigir la información? ¿O simplemente los que le temen a perder su intimidad deben abstenerse de utilizar el Internet?

Esta investigación intenta resolver el problema de la falta de protección constitucional para la intimidad en Internet. Ya que el Internet es un fenómeno relativamente reciente, son contadas las veces en que el Tribunal Supremo de Estados Unidos se ha expresado al respecto. Por su parte, el Tribunal Supremo de Puerto Rico aun no se ha expresado sobre este tema. A través de un análisis jurisprudencial y estatutario del estado de Derecho que actualmente rige el mundo cibernético, este trabajo de investigación señala las lagunas existentes y recomienda un esquema legal para cuando surja la eventualidad de que nuestro más alto Foro se tenga que expresar al respecto. Además, establece la necesidad de que el Gobierno respete los derechos básicos de intimidad al inmiscuirse en la recopilación de información a través de Internet.

La primera parte de este trabajo explicará cómo opera el Internet y la facilidad que hay para recopilar datos personales de los usuarios. La segunda parte se enfocará en el alcance del derecho a la intimidad en Estados Unidos, España[2] y Puerto Rico. Por medio de un análisis entre las tres jurisdicciones se intentará descifrar si las garantías constitucionales que protegen la intimidad se extienden al Internet. En particular, se explicará el desarrollo de la doctrina prevaleciente en cada jurisdicción al enfrentarse a una controversia entre intimidad y comunicaciones. En la tercera parte del trabajo se demostrará la aplicación de la protección de la intimidad al ámbito cibernético. En específico, se discutirán las leyes aplicables en cada jurisdicción y cómo los tribunales han atacado una controversia entre el Internet y el derecho a la

---

[2] Se ha escogido la jurisdicción española por su afinidad a la puertorriqueña en su valoración del derecho a la intimidad. Para los fines del análisis, se utilizará la jurisprudencia emitida por el Tribunal Constitucional de España.

intimidad. Por último, se recomendará la adopción de un esquema jurídico en Puerto Rico que manifieste nuestra alta valoración del derecho a la intimidad.

II. La recopilación de datos personales en Internet

El Internet es un espacio cibernético que accedemos a través de nuestras computadoras y teléfonos móviles para diversos propósitos. Irónicamente, el Internet es para muchos una dimensión paralela donde existe la posibilidad de mantener una vida en secreto, ya sea a través del anonimato o por el mero hecho de que no tienen que salir de sus hogares para interactuar con otros. Parece ser un mundo fuera del escrutinio público. Sin embargo, la realidad es que, al acudir al Internet, nos exponemos inconscientemente a una vigilancia constante, donde entidades privadas, así como el Gobierno, pueden rastrear cada movimiento nuestro.

El Internet facilita el acceso a datos personales a través de tecnología que monitorea la actividad de los usuarios. Los datos de la secuencia de clic (*clickstream data*) consisten en la información recopilada cuando un usuario navega el Internet.[3] La información obtenida sirve para crear un perfil de las transacciones y comunicaciones de un usuario, así como las páginas web visitadas y las compras hechas. La dirección de protocolo (*I.P.*, por sus siglas en inglés) le asigna un número de identificación a cada usuario de Internet y el mismo puede ser rastreado para conseguir al dueño de la computadora. Asimismo, hay fragmentos de información (*cookies*) que se almacenan en el disco duro del visitante de una página web a través de su navegador.[4] Al llenar una suscripción a través del Internet, la información sometida voluntariamente puede ser accedida por los operadores de la página web para relacionarla con los *cookies* e identificar a la persona.[5]

La tecnología actual hace posible mantener un registro de cada página visitada por un usuario para así crear perfiles detallados de cada navegante.[6] Los datos recopilados, en la mayoría de los casos, son utilizados para propósitos de mercadeo y publicidad, ya que si una compañía privada adquiere conocimiento sobre las páginas que un usuario accede, puede inferir cuáles son sus preferencias y así mostrarle publicidad que sea de su interés.[7] De igual manera, los motores de búsqueda, como Google, acostumbran recopilar datos de sus usuarios con un propósito supuestamente

---

[3] Madeleine Schachter, *Law of Internet Speech* cap. 4, 431 (2da ed., Carolina Academic Press 2002).

[4] *Id*.

[5] *Id*.

[6] Coral Rodríguez Morales, Autor Estudiante, *El Internet y la protección del derecho a la intimidad*, 72 Rev. Jurídica U.P.R. 805, 807 (2003).

[7] Un ejemplo clásico del uso de esta tecnología son las recomendaciones de libros que hace Amazon a sus clientes basadas en su historial de consumo. De igual manera, el motor de búsqueda Google emplea esta tecnología para mostrarle al usuario publicidad y resultados conforme a sus preferencias. Google Watch-Watch, *The Big G & Privacy*, http://www.google-watch-watch.org/privacy.php (accedido el 9 de marzo de 2010).

legítimo. El reconocido motor de búsqueda acostumbra leer los mensajes que cada usuario envía y recibe e identifica palabras claves para así presentarle anuncios y resultados de búsqueda conforme a sus intereses y preferencias. Además, Google retiene cada mensaje, incluso los ya borrados por el usuario. La explicación para recopilar esta información es que facilita la experiencia del usuario en su página ya que los resultados de búsqueda van a estar dirigidos a cada navegante.

A pesar de que las compañías que recopilan datos tienden a establecer en su política de privacidad que no le venden la información a terceras personas, eso no les impide de proveerle la información al gobierno si se la exige mediante *subpoena*.[8] Por lo tanto, no hay límites a la recopilación de información que tiene el potencial de ser usada en contra de las personas. Ante esta realidad, el universo totalitarista *orwelliano* parece cobrar vigencia y nos enfrentamos a la posibilidad de perder toda noción de intimidad en Internet.

III. El potencial para violaciones al derecho a la intimidad

Al momento, la tendencia de las compañías privadas es irse aliando con el gobierno para brindarle acceso a los datos personales que recopilan a través del Internet. Al Gobierno de Estados Unidos le interesa dicha información para propósitos de seguridad nacional, en especial después de los ataques terroristas del 11 de septiembre de 2001. A manera de ejemplo, Google está negociando con la Agencia de Seguridad Nacional del Departamento de Defensa (N.S.A., por sus siglas en inglés) un acuerdo para compartir datos. El acuerdo tiene el propósito de proteger a Google pero, debido a las tácticas de espionaje del N.S.A., la alianza entre ambas entidades hace peligrar la intimidad de los ciudadanos.[9]

De manera similar, La Oficina de Administración y Presupuesto (O.M.B., por sus siglas en inglés) ha propuesto permitir el uso de tecnología de rastreo en el Internet en páginas del gobierno federal. Desde el 2000, el gobierno federal no usaba dicha tecnología. El permitir el rastreo puede contribuir a la formación de una base de datos que incluya los historiales de visita de los usuarios, así como la información que comparten en la página. Como los usuarios de la red acostumbran a proveer su nombre y dirección de correo electrónico, la tecnología de rastreo permite asociar el nombre con los hábitos de navegación.[10] Las violaciones a la intimidad del ciudadano debido a acuerdos que se hacen con el gobierno serán más frecuentes en un futuro.

---

[8] Zach Viglianco, The Daily Athenaeum, *With New Technologies, Google may become your 'Big Brother'*, http://www.thedaonline.com/opinion/with-new-technologies-google-may-become-your-big-brother-1.1223247 (accedido el 4 de marzo de 2010).

[9] A.C.L.U., *Tell Google Not to Enter Into An Agreement With the NSA*, http://www.aclu.org/technology-and-liberty/tell-google-not-enter-agreement-nsa (accedido el 5 de marzo de 2010).

[10] A.C.L.U., *Government Proposes Massive Shift in Online Privacy Policy*, http://www.aclu.org/free-speech_technology-and-liberty/govt-proposes-massive-shift-online-privacy-policy (accedido el 10 de agosto de 2009).

Ante esa facultad irrestricta del gobierno a acceder información, se va viendo la necesidad que tienen los tribunales y la legislatura de decidir cómo se enfrentarán a una controversia de este tipo.

IV. El derecho a la intimidad y la regulación actual del Internet

A. Estados Unidos

El reconocimiento del derecho a la intimidad posiblemente se originó en un artículo de Revista Jurídica[11] que data de 1890 donde se formuló la primera doctrina sobre dicho derecho.[12] Debido a que no hay un derecho explícito a la intimidad en la Constitución de Estados Unidos el mismo proviene de las "penumbras" de la Constitución.[13] No obstante, el Tribunal Supremo de los Estados Unidos ha resuelto que hay ciertas áreas donde existe un interés para garantizar intimidad. Entre esas áreas, la Constitución en su Cuarta Enmienda protege a los ciudadanos de registros y allanamientos irrazonables a los fines de que sólo será razonable un registro cuando el mismo esté acompañado de una orden judicial expedida a base de causa probable.[14] Desde un punto de vista constitucional, la protección más clara y poderosa a la intimidad la ofrece la prohibición de la Cuarta Enmienda contra registros y allanamientos irrazonables.[15]

Aún no se ha aclarado si la Cuarta Enmienda Federal protege la información que surge de la navegación del Internet, independientemente del tipo de información que sea. Esto se debe a que la escasa jurisprudencia federal que atiende el derecho cibernético siempre hace una distinción entre información de tipo contenido y de no contenido para determinar la aplicación de la Cuarta Enmienda.

El esquema legal básico establecido para garantizar la intimidad prohíbe el acceso a información personal derivada de las comunicaciones de una persona sin una orden judicial expedida a base de causa probable.[16] No obstante, como primer paso para determinar si la Cuarta Enmienda Federal cobija la información rastreada, se debe determinar si el usuario de Internet tiene una expectativa razonable de intimidad sobre dicha información.

---

[11] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 193-220 (1890) ("[t]hat the individual shall have full protection in person and property is a principle as old as the common law; but it has been found necessary from time to time to define anew that exact nature and extent of such protection.").

[12] Luis D. Rosa Velázquez, Autor Estudiante, *Panorama general del Derecho a la Intimidad*, 72 Rev. Jurídica U.P.R. 665, 672 (2003).

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

[14] Const. EE. UU. Enmienda IV, § 2.

[15] Raymond S. R. Ku & Jacqueline Lipton, *Cyberspace Law* cap. 5, 582 (3ra ed., Aspen Publishers 2010).

[16] *Katz v. United States*, 389 U.S. 347, 358-59 (1967).

i. La expectativa razonable de intimidad federal

Para que exista la protección constitucional en cualquier ámbito, tiene que determinarse que hay tanto una expectativa de intimidad subjetiva como una objetiva. Es decir, en primer lugar, se debe evaluar "si la persona agraviada, en su subjetividad y en las circunstancias en que se encuentra, puede reclamar un derecho de intimidad".[17] Si se encuentra que existe una expectativa subjetiva, entonces se pasa a evaluar la expectativa objetiva; es decir, "si la sociedad está dispuesta a reconocer si [ese] reclamo de intimidad debe estar protegido",[18] Sólo cuando concurra una expectativa objetiva y una subjetiva se puede hablar de una expectativa razonable de intimidad. A pesar de que el estándar clásico es el de la expectativa razonable de intimidad, le ha sido difícil a los tribunales federales determinar qué constituye una expectativa razonable de intimidad en el mundo virtual.[19] La jurisprudencia federal contradictoria demuestra esta dificultad. En una ocasión, se denegó una moción de supresión de evidencia basado en que no había protección constitucional bajo la Cuarta Enmienda sobre información que se provee para propósitos de suscripción.[20] En otra ocasión, se resolvió que una persona tiene una expectativa razonable de intimidad con la información contenida en una cuenta de punto de conexión con un servidor electrónico (en lo sucesivo I.S.P., por sus siglas en inglés), al amparo de la Constitución de New Jersey.[21]

No todos los casos que se han visto en los tribunales han llegado a la misma conclusión. Unos pocos han resuelto que el derecho a la intimidad es oponible frente a aquellas entidades que desean acceder información recopilada a través de Internet, por existir una expectativa razonable de intimidad en Internet. En *United States v. Maxwell*, se encontró que el contenido de las conversaciones de correo electrónico sugería que ambas partes tenían una expectativa de que las conversaciones eran privadas.[22] De igual manera, en *Warshak v. United States*, se encontró una expectativa razonable de intimidad en comunicaciones a través de correo electrónico porque el ISP no acostumbraba a grabar el contenido del correo electrónico en el transcurso ordinario del negocio.[23] Asimismo, en *United States v. Heckenkamp* se resolvió que

---

[17] Carlos E. Ramos González, Ponencia, *La inviolabilidad de la dignidad humana: lo indigno de la búsqueda de expectativas razonables de intimidad en el derecho puertorriqueño* (San Juan, P.R.) (28 de octubre de 2010) (copia disponible en http://academiajurisprudenciapr.org/revistas/2010/discurso-del-academico-de-numero-carlos-e-ramos-gonzalez/).

[18] *Id*.

[19] El Tribunal Supremo Federal estableció que: "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as *reasonable*." *Katz*, 389 U.S. 347 (Harlan, J., concurrente).

[20] *United States v. Cox*, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002).

[21] *State v. Reid*, 914 A. 2d 310 (N.J. Super. Ct. App. Div. 2007).

[22] 45 M.J. 406, 417 (1996).

[23] 490 F.3d 455 (6to Cir. 2007).

un estudiante tiene una expectativa razonable de intimidad en la información que transmite a través de la red de la universidad debido a que no había ninguna política de monitoreo anunciada.[24]

Desafortunadamente, el análisis de protección constitucional en el ámbito federal no acaba con la expectativa de intimidad. Además, para aplicar la Cuarta Enmienda los tribunales exigen que se haga una distinción entre información de tipo contenido y de tipo no contenido. Este segundo paso del análisis disminuye la posibilidad de que un reclamo contra la intimidad prevalezca.

ii. La distinción contenido y no contenido

La distinción entre lo que es información de contenido y de no contenido es indispensable para determinar si aplica la protección constitucional de la Cuarta Enmienda Federal. La dirección de una página web, por ejemplo, es información tipo contenido ya que de la misma se desprende el contenido de la página visitada, así como lo que el usuario buscó en dicha página. Por su parte, la dirección a la cual se envía un correo electrónico no es de contenido porque de la misma lo único que se podría acceder es el nombre del usuario suscrito al I.S.P.[25]

Como regla general, la Cuarta Enmienda protege la información de tipo contenido, pero en el ámbito de la información que surge navegando el Internet, no es tan fácil descifrar lo que constituye contenido. Por ejemplo, no se encontró una expectativa de intimidad en cuanto a los números llamados con un teléfono porque se esperaba que la compañía telefónica tuviera acceso a dicha información.[26] De igual forma, un empleado no tiene una expectativa legítima de intimidad en cuanto al registro que mantenía su patrono de su uso del Internet.[27]Para entender a cabalidad de dónde se origina en Estados Unidos el derecho a la intimidad sobre el control de información, hay que examinar tres casos que desarrollaron la doctrina prevaleciente: *Katz v. United States,*[28] *United States v. Miller*[29] y *Smith v. Maryland.*[30]

iii. Jurisprudencia federal aplicable

a. *Katz v. United States*

Hay dos acercamientos a la protección que ofrece la Cuarta Enmienda. El primero equivale a un requerimiento de información a través de un registro o allanamiento

---

[24] 482 F.3d 1142, 1147 (9no Cir. 2007).

[25] Matthew J. Tokson, *The Content/Envelope Distinction in Internet Surveillance Law*, 50 Wm. & Mary L. Rev. 2105, 2158 (2009).

[26] *Smith v. Maryland*, 442 U.S. 735, 742 (1979).

[27] *United States v. Simons*, 206 F. 3d 392 (4to Cir. 2000).

[28] 389 U.S. 347 (1967).

[29] 425 U.S. 435 (1976).

[30] 442 U.S. 735 (1979).

irrazonable. El segundo requiere un traspaso físico a una zona de intimidad. En *Katz* el Tribunal Supremo resolvió que la Cuarta Enmienda protege a personas, no a lugares, y por lo tanto lo que una persona expone al público conscientemente, aunque sea en su hogar u oficina, no está sujeto a la protección de la Cuarta Enmienda. En este caso, una persona había sido convicta por transmitir información sobre apuestas entre estados a través del teléfono, en violación de una ley federal. Sin embargo, lo que se desea mantener privado, aunque sea en un área de acceso público, puede estar sujeto a protección constitucional al amparo de la Cuarta Enmienda, si se logra demostrar que hay una expectativa razonable de intimidad.[31] Una expectativa de intimidad subjetiva es legítima si es una que la sociedad está dispuesta a reconocer como razonable.[32]

Katz se convirtió en el caso doctrinal para la intimidad en Internet. Sin embargo, para la década de los 1970, el Tribunal Supremo debilitó la protección a la intimidad que había interpretado *Katz,* en el sentido que resolvió que cuando la información personal está en manos de terceros, como lo sería en el caso de Google, la expectativa de intimidad es menor.[33] A continuación se discuten los dos casos que debilitaron, y a su vez desarrollaron, la doctrina de *Katz*.

b. *United States v. Miller*

El Tribunal Supremo Federal resolvió en *Miller* que un *subpoena* para requerirle información al banco no era un registro porque no existía una expectativa razonable de que la información en el banco fuera privada. El Tribunal razonó que cuando se revela información a una tercera persona, el sujeto asume el riesgo de que la información se le revele al gobierno. Esto aplica aunque se le haya revelado la información bajo una presunción de confiabilidad o uso limitado. Una vez se revela la información personal, aunque sea como un privilegio confidencial entre un banco y el cliente, el cliente pierde su expectativa de intimidad y no le debe sorprender si la información pasa a manos de terceras personas.[34]

c. *Smith v. Maryland*

Tres años después, el Tribunal resolvió que no hay una expectativa de intimidad razonable en los archivos de las llamadas realizadas porque se espera que las compañías telefónicas tengan acceso a los números marcados. En este caso, se

---

[31] *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).

[32] *Minnesota v. Olson*, 495 U.S. 91, 95-96 (1990).

[33] Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 Utah L. Rev. 1433, 1471.

[34] Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1402 (2004).

extendió la doctrina de asunción de riesgo al efecto de que un individuo carece de una expectativa razonable de intimidad en los números telefónicos que marca. Sin embargo, el Tribunal hizo una distinción al resolver *Smith,* a los efectos de que un número de teléfono no es información de contenido. Por lo tanto, la protección de la Cuarta Enmienda aplica, siempre y cuando, la información que esté en manos de terceros sea de tipo contenido. Si no hay contenido involucrado, no hay protección constitucional.[35]

Los tribunales también han extendido la doctrina de asunción de riesgo a circunstancias cuando se revela información personal a terceros, quienes a su vez le revelan dicha información al gobierno.[36] Incluso, los tribunales han autorizado el acceso del gobierno, sin orden judicial, a los récords de ISP de los clientes que incluye información como nombre, dirección, fecha de nacimiento y contraseñas.[37] El Tribunal de Apelaciones del Noveno Circuito ha aplicado la doctrina de *Miller* a un requerimiento del gobierno para información adicional de un cliente suscrito al servicio de ISP, incluyendo a quién le envió correos electrónicos y el historial de páginas visitadas (basados en su dirección I.P.). El Tribunal determinó que ese tipo de información era idéntica a aquella utilizada en *Smith* por ser información que no revela contenido. Por lo tanto, si la información hubiera sido una que revele más acerca de la identidad de la persona, entonces sería de contenido y requeriría mayor protección constitucional. na lista de las direcciones de las páginas visitadas por las personas (U.R.L.), por ejemplo, hubiera sido información de tipo contenido.

En síntesis, la doctrina de asunción de riesgo de *Smith* aplica cuando el gobierno intenta acceder información de no contenido. *Katz* y la expectativa razonable de intimidad sigue aplicando cuando la información es de contenido. A raíz de estos dos casos, el gobierno tiene prácticamente una facultad irrestricta de exigir información en manos de terceros sin tener que preocuparse de una violación a la Cuarta Enmienda.[38] Debido a que casi toda la información que se recopila a través de la cosecha de información (*data mining*) se le vende a compañías privadas, el Gobierno no se enfrenta a problemas constitucionales.

---

[35] El Juez Stewart disiente y argumenta que los números de teléfonos, para efectos de la distinción, son de contenido porque a través de ellos se puede fácilmente obtener la identidad de las personas.

[36] *United States v. Jacobsen*, 466 U.S. 109 (1984) (un paquete de drogas enviado a través de Federal Express); *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984) (récords financieros en manos del corredor de bolsas); *California v. Greenwood*, 486 U.S. 35 (1988) (bolsas de basura en la acera); *United States v. Phibbs*, 999 F.2d 1053 (6to Cir. 1993) (estados de cuenta de tarjetas de crédito y récords de teléfonos).

[37] *Véase Guest v. Leis*, 255 F.3d 325 (6to Cir. 2001); *United States v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000); *United States v. Hambrick*, 55 F.Supp.2d 504 (4to Cir. 2000); *United States v. Cox*, 190 F. Supp.2d 330, 332 (N.D.N.Y. 2002); *United States v. Bach*, 310 F.3d 1063 (8vo Cir. 2002).

[38] Cristopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. Chi. L. Rev. 317 (2008).

iv. Leyes federales aplicables

Actualmente, la jurisdicción federal cuenta con un esquema legal insuficiente para proteger el derecho de la intimidad del ciudadano en el Internet. Conforme al análisis anteriormente explicado, la Cuarta Enmienda no es suficiente porque la misma se torna irrelevante una vez se determina que no hay expectativa de intimidad. Ante la falta de protección constitucional, acudimos a los estatutos que rigen las comunicaciones en Estados Unidos. La Ley Federal de Comunicaciones de 1934 fue la primera ley sobre el rastreo electrónico de las telecomunicaciones.[39] Debido a su cubierta limitada, en 1968 se aprobó el Título III del *Omnibus Crime Control and Safe Sreets Act* [40], que precisó la definición de interceptación a la adquisición auditiva de comunicación a través de un aparato electrónico. A su vez, no prohibió terminantemente la interceptación, sino que la autorizó previo el consentimiento de al menos una de las partes envueltas en la comunicación.

Posteriormente, el estatuto principal en esta área de Derecho fue el *Electronic Communications Privacy Act* (en lo sucesivo E.C.P.A.).[41] El E.C.P.A. se aprobó en 1986 como una enmienda al *Omnibus Crime Control and Safe Streets Act* y recogió el Título III. Evidentemente, en el 1986 el Internet no contaba con el auge de hoy día, así que parecería lógico que la ley fuera insuficiente. La ley se aprobó con el propósito de proteger la intimidad frente a los adelantos tecnológicos de la época. Sin embargo, muchas de las tecnologías que la ley establece ya están extintas hoy. La ley consiste de tres estatutos: el *Wiretap Act*[42], el *Pen Register Act*[43] y el *Stored Communications Act*[44] (en lo sucesivo S.C.A.). De estos tres, el más pertinente a la intimidad de los usuarios de Internet es el S.C.A. Vale aclarar que el E.C.P.A.[45] extiende las restricciones gubernamentales sobre la intervención en líneas telefónicas para incluir la data electrónica transmitida por una computadora. Sin embargo, la E.C.P.A. sólo protege las comunicaciones mientras están en tránsito. Esto implica que la E.C.P.A. no aplica a las comunicaciones en Internet, ya que los mensajes que se transmiten a través de Internet se detienen y se guardan múltiples veces de camino a su destino.

En 1980 se promulgó el *Electronic Funds Transfer Act*[46] que "provee un aviso para el descubrimiento rutinario a terceras personas de expedientes personales hechos por una transferencia automática de dinero".[47] En lo pertinente a nuestra área

---

[39] 47 U.S.C. § 605 (2009).

[40] 18 U.S.C. §§ 2510-22 (2009).

[41] 18 U.S.C. §§ 2510-22 (2009).

[42] 18 U.S.C. §§ 2510-2522 (2009).

[43] 18 U.S.C. §§ 3121-3127 (2009).

[44] 18 U.S.C. §§ 2701-2711 (2009).

[45] 18 U.S.C. §§ 2510-2521, 2701-2711, 3121-3127 (2009).

[46] 15 U.S.C. §§ 1693-93r (2009).

[47] Rosa Velázquez, *supra* n. 8, en la pág. 687.

de investigación, en 1984 se aprobó el *Cable Communications Policy Act*[48], que le exige a los operadores de cable avisar sobre prácticas de recopilación de información personal identificable y le brinda a los clientes el "derecho de acceder sus expedientes y un derecho general de optar por prohibir la divulgación de información más allá de la necesaria para proveer el servicio de cable".[49] Después de los ataques terroristas de septiembre de 2001, se aprobó el *U.S.A. Patriot Act*[50] que limita el poder de las personas para controlar su información personal. Se deterioró el derecho a la intimidad debido al interés apremiante del Estado por velar por la seguridad nacional y ofrecer protección contra el terrorismo.

La postura federal en cuando a la protección del derecho a la intimidad en el ámbito cibernético es una que fomenta la transparencia del proceso, en vez de enfocarse en la prohibición de la recopilación de datos. Incluso, la tendencia a través de los estados es de fomentar la transparencia del proceso. En California, por ejemplo, se ha implementado el *Online Privacy Protection Act* que exige que aquellas entidades que recopilen datos personales a través del Internet, tengan una política de privacidad identificando el tipo de data que recopilan y terceras personas con quienes los pueden compartir. De manera similar, hay otros quince estados que requieren, por ley, que se publiquen expresamente las políticas de privacidad en las páginas web.[51] Sólo Nevada y Minnesota exigen que no se divulguen los datos personales de sus usuarios, a menos que el usuario consienta expresamente a que se publiquen sus datos.[52]

Con la publicación de políticas de privacidad anunciando la posibilidad de vender la información a terceras personas, las compañías y el Gobierno evitan asumir responsabilidad por los datos personales. Los usuarios, por su parte, se ven forzados a renunciar a su derecho a la intimidad cuando acceden el Internet ya que se valoriza más el acceso a información que la protección de los datos personales de cada ciudadano.

B. España

i. El nuevo derecho fundamental a la protección de datos

El derecho a la intimidad en España está contemplado en el Artículo 18 de la Constitución Española como uno fundamental. El mismo "garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen", así como, "el secreto

---

[48] 47 U.S.C. § 551 (2009).

[49] Rosa Velázquez, *supra* n. 8, en la pág. 688.

[50] U.S.A. Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[51] National Conference of State Legislatures. *State Laws Related to Internet Privacy*. (actualizado el 19 de octubre de 2009). http://www.ncsl.org/default.aspx?tabid=13463. (accedido el 5 de octubre de 2010).

[52] *Id*.

de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".[53] Además, en su último apartado, establece que "[l]a 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". (Énfasis suplido).[54] La Constitución divide el derecho a la intimidad en cuatro vertientes: (1) la personal, como lo serían la honra y la propia imagen; (2) la relacionada al domicilio y al registro; (3) la que busca el secreto de las comunicaciones; y (4) la que limita el uso de la informática. Cada una de estas vertientes es subsidiaria, por lo cual una violación al derecho a la intimidad puede que no necesariamente conlleve una violación al secreto de comunicaciones.[55]

Una simple lectura del Artículo 18 nos revela que la Constitución Española le ofrece a los ciudadanos unos derechos que nuestra Constitución jamás ha ofrecido expresamente. Ambas disposiciones antes mencionadas anticipan que el derecho a la intimidad español se podría conciliar más fácilmente, desde un punto de vista constitucional, con la moderna tecnología de recopilación de datos personales en Internet. El apartado pertinente a la informática (el 18.4) fue incluido expresamente para "prevenir posibles abusos en la utilización de la informática, que menoscabaran el ejercicio de las libertades".[56] El mismo tiene dos aspectos:

> [U]no, es de significación *negativa* y se traduce en el derecho a no hacer de dominio público ciertas informaciones de carácter personal, privado o reservado; el otro, es *positivo* e implica el ejercicio de un derecho al control de datos concernientes a la propia persona que han rebasado la esfera de la [intimidad] para devenir elementos de [la entrada de información] de un programa electrónico.[57]

Ya desde su incorporación en 1978 el ordenamiento español venía contemplando la idea de que "al desafío de la técnica no se debe responder sólo con la técnica".[58] Se entendía que se respondía de mejor manera garantizando el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona, provenientes de un uso ilegítimo del tratamiento mecanizado de datos.[59]

---

[53] Artículo 18 de la Constitución Española de 1978.

[54] *Id*.

[55] Eliseu Frígolsi Brines, *La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías*, en Javier Boix Reig & Ángeles Jareño Leal, *La protección jurídica de la intimidad* 37, 50 (Iustel 2010).

[56] Antonio E. Pérez Luño, *Informática y libertad: Comentario al Artículo 18.4 de la Constitución*, 24 Rev. Estudios Políticos 31, 44 (1981).

[57] Pérez, *supra* n. 56, en la pág. 45.

[58] *Id*. en la pág. 53 citando a J. Habermas, *Technikund Wissenschaftais Ideologie* 118 (Frankfurt 1968).

[59] Sentencia del Tribunal Constitucional, S.T.C. No. 292/2000 de 30 de noviembre.

Debido a las cuatro vertientes que la caracterizan, una violación al derecho a la intimidad español necesariamente requiere un análisis del contenido de lo que alegadamente viola la intimidad. De esta manera, se ha adoptado una postura similar a la estadounidense al enfrentarse a una violación del derecho a la intimidad. En cuanto a aquellas violaciones relacionadas al secreto de las comunicaciones contemplado en la Constitución, se ha establecido que:

> [P]ara considerar si se vulnera el derecho fundamental a la intimidad resulta absolutamente necesario acudir al contenido de aquello de lo que se predica su pertenencia al ámbito íntimo o privado, en lo que el Tribunal Constitucional denomina dimensión material del secreto.[60]

El examen del contenido de la comunicación es esencial para determinar si la revelación hecha a terceros viola el derecho a la intimidad autónomo o el secreto de las comunicaciones.[61]No obstante, el marco jurídico español se diferencia del estadounidense en la nueva vertiente del derecho a la intimidad que crearon. A través de recursos que se fueron ventilando en el Tribunal Constitucional de España, la nación española presenció una configuración jurisprudencial del nuevo derecho fundamental a la protección de datos personales por medio de un conjunto de sentencias que comienzan con la S.T.C. 254/1993 y culminan con la S.T.C. 292/2000. Se creó un derecho de control sobre los datos relativos a la propia persona que trasciende el ámbito del derecho fundamental a la intimidad.[62] "La llamada *libertad informática* es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".[63]

El derecho fundamental a la protección de datos difiere del derecho de la intimidad en que le otorga a su titular el poder de imponer a terceros determinados comportamientos regulados por la Ley de Protección de Datos, la cual fue implementada en 1999.[64] El derecho a la protección de datos "persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado".[65] Mientras que el derecho a la intimidad protege "frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad".[66] El derecho fundamental a la protección de datos:

---

[60] *Id*. en la pág. 42.
[61] *Id*. en la pág. 43.
[62] S.T.C. 292/2000.
[63] S.T.C. 292/2000.
[64] Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal de España.
[65] S.T.C. 292/2000.
[66] *Id*.

> [A]mplía la garantía constitucional a aquellos de esos datos que sean relevantes para . . . los derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.[67]

Protege todo tipo de datos porque su objeto no es sólo la intimidad individual sino la protección de datos de carácter personal. Por tal razón, dicho derecho también alcanza los datos personales públicos.

El derecho a la protección de datos ha tenido dos grandes repercusiones en el ámbito cibernético. Por un lado, ha facultado al ciudadano a saber en todo momento quién dispone de sus datos personales y a qué uso los está sometiendo. Por otro lado, le ha dado el poder de oponerse a la posesión y usos de los datos.

ii. La Agencia Española de Protección de Datos

Con la creación del derecho a la protección de datos personales, nació además la Agencia Española de Protección de Datos (en adelante "A.E.P.D."). La misma es una entidad pública e independiente que está encargada de velar en España por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal. Su función general es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial, lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.[68] La agencia tiene la facultad de ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de datos, así como ejercer una potestad sancionadora.[69]

La facultad que la A.E.P.D. tiene para sancionar demuestra la intención española de acabar con el uso ilegal de datos personales recopilados a través de Internet. A manera de ejemplo, en el 2007, la Agencia emitió una resolución ordenando a Google a excluir los datos personales de un usuario de los índices elaborados por Google.[70] La Agencia hizo dicha determinación basándose en el derecho a la protección de datos y la libertad informática, que le permite al ciudadano oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención.

---

[67] *Id*.

[68] *Agencia Española de Protección de Datos*, http://www.agpd.es/portalwebAGPD/conozca/funciones/index-ides-idphp.php (accedido el 20 de octubre de 2010).

[69] *Id*.

[70] Resolución No. R/01046/2007 de 20 de noviembre de la Agencia Española de Protección de Datos.

C. Puerto Rico

La Constitución de Puerto Rico le ofrece mayor protección a la intimidad que la Constitución Federal. En la primera disposición al respecto, la Constitución establece que la dignidad del ser humano es inviolable.[71] Además, dispone que las personas tienen derecho a protección contra ataques a su honra, su reputación y a su vida privada o familiar.[72] De esta manera, la disposición es muy similar al derecho a la intimidad español.

El derecho a la intimidad en Puerto Rico es "de factura más ancha" que el de Estados Unidos, ya que consta expresamente en la Constitución. Además, el mismo opera *ex proprio vigore* e incluso puede hacerse valer frente a personas privadas.[73] El derecho a la intimidad en Puerto Rico es de la más alta jerarquía, aunque no es absoluto. El mismo se mantiene en lucha constante entre lo privado y lo colectivo, lo interno y lo externo, entre la libertad y la seguridad.[74]

Debido a que la dignidad del ser humano es un asunto tan central en el derecho a la intimidad puertorriqueño, un reclamo de intimidad en Puerto Rico debe "extenderse a aquellas nociones expresivas más amplias relativas al control sobre la proyección de la identidad".[75] De tal manera, el derecho a la intimidad puertorriqueño incluiría el "control sobre la información personal aún cuando la misma haya sido revelada".[76] En otras palabras, el criterio para determinar si se viola el derecho a la intimidad constituiría en evaluar si el individuo conserva la capacidad para controlar la proyección de identidad a través del control de información personal.[77]

El alcance del derecho a la intimidad en Puerto Rico tuvo un gran adelanto cuando se prohibió expresamente en la Constitución[78] interceptar llamadas telefónicas[79] Pero la extensión de este derecho sobre las comunicaciones en el Internet no se ha aclarado. Simplemente, el Tribunal Supremo ha interpretado que la prohibición de interceptar llamadas telefónicas no es absoluta, ya que hay circunstancias excepcionales, como el hostigamiento, que permiten la interceptación.[80]

---

[71] Const. P.R. Art II, § 1, "La dignidad del ser humano es inviolable".

[72] Const. P.R. Art. II, § 8, "Toda persona tiene derecho a protección de ley contra ataques abusivos a su honra, su reputación y a su vida privada o familiar".

[73] *Arroyo v. Rattan Specialties*, 117 D.P.R. 35, 64 (1986); *Puerto Rico Tel. Co. v. Martínez*, 114 DPR 328, 339 (1983).

[74] Rosa Velázquez, *supra* n. 8, en la pág. 665.

[75] Hiram A. Meléndez Juarbe, *La Constitución en ceros y unos: Un acercamiento digital al Derecho a la Intimidad y la seguridad pública*, 77 Rev. Jurídica U.P.R. 45, 75 (2008).

[76] *Id*.

[77] *Id*.

[78] Const. P.R. Art. II, §10, "No se interceptará la comunicación telefónica".

[79] Arlene de Jesús Martínez, Autor Estudiante, *El Derecho a la Intimidad y las telecomunicaciones*, 71 Rev. Jurídica U.P.R. 761, 762 (2003).

[80] *P.R.T.C. v. Martínez*, 114 D.P.R. 328, 359 (1983).

En Puerto Rico la jurisprudencia se limita a establecer el desarrollo del derecho a la intimidad en las telecomunicaciones. El Tribunal Supremo no se ha expresado sobre el derecho a la intimidad en Internet. Veamos algunos casos donde el Tribunal Supremo demuestra su inclinación a permitir las telecomunicaciones por encima del derecho a la intimidad. En *Pueblo v. Luzón*,[81] los acusados alegaron en apelación que la evidencia era inadmisible ya que se habían tomados retratos y películas en movimiento, en lugares protegidos contra intromisiones indebidas del Estado.[82] El Tribunal permitió la evidencia luego de razonar que los acusados no gozaban de una expectativa razonable de intimidad.

En *P.R.T.C. v. Martínez*,[83] las demandadas recibieron llamadas de hostigamiento que perturbaban su tranquilidad mental. A pesar de que la Constitución prohíbe la interceptación de llamadas telefónicas, el Tribunal permitió la interceptación, catalogando la situación como una excepcional, ya que había consentimiento de la dueña del teléfono. El Tribunal aclaró que el derecho a la intimidad en esta esfera sólo tiene de absoluto "el albedrío que tiene el ciudadano para reclamar del Estado y los tribunales de hacer valer el respeto a la expectativa legítima de intimidad que rodea su comunicación telefónica".[84] En *Vega Rodríguez v. P.R.T.C.* el Tribunal Supremo resolvió, bajo la misma tendencia, que los mecanismos de vigilancia electrónica en el lugar de trabajo no son inconstitucionales y el mero hecho de utilizarlos no constituye una intromisión inaceptable en la intimidad del empleado.[85] La utilización de estos equipos de vigilancia en este caso fue constitucional pues P.R.T.C. logró demostrar que tenía intereses apremiantes que atender, como lo son su seguridad y el óptimo funcionamiento del sistema de comunicaciones de Puerto Rico.[86]

Por último, es menester recalcar un caso que, aunque no versa sobre las telecomunicaciones, reconoce la importancia de la intimidad al momento de revelarle información personal a terceros. Se trata del caso de *Rodríguez v. Scotiabank*[87] donde nuestro Tribunal Supremo expresamente rechazó la doctrina federal de *United States v. Miller* y estableció que ante solicitud de descubrimiento de las copias de planillas de contribución de un individuo, nuestro derecho a la intimidad prohíbe que las mismas sean "objeto de descubrimiento indiscriminado."[88]

---

[81] 113 D.P.R. 315 (1982).

[82] 113 D.P.R. 315, 325 (1982).

[83] 114 D.P.R. 328 (1983).

[84] *Id*. en la pág. 343.

[85] 152 D.P.R. 584 (2002).

[86] La decisión tomada es consistente con otras opiniones del T.S.P.R. *Véase U.T.I.E.R. v. A.E.E.*, 149 D.P.R. 498 (1999) (se permitió interceptar teléfonos para mejorar la calidad de servicio) y *Pueblo v. Colón Raffucci*, 139 D.P.R. 959 (1996) (la acción del Policía de mantener un celular encendido no constituye una interceptación telefónica).

[87] 113 D.P.R. 210 (1982).

[88] *Id*. en la pág. 221.

Es evidente que la tendencia en Puerto Rico es permitir la interceptación de llamadas telefónicas en contravención a las disposiciones constitucionales que lo prohíben. En la jurisprudencia discutida, los intereses del Estado van por encima del derecho la intimidad. Siendo el derecho a la intimidad uno de tan alta jerarquía en nuestro ordenamiento resulta contradictorio que muchas veces se obvie. Como no ha surgido un caso sobre el tema de Internet en Puerto Rico, habría que especular sobre la inclinación del Tribunal Supremo, de surgir algún día un caso en este área. La tendencia de los tribunales parece indicar que no prevalecería la intimidad. Sin embargo, lo primero que se debe verificar es si en efecto los usuarios de Internet poseen una expectativa razonable de intimidad. Una vez determinado que sí la poseen, se debe proseguir con el análisis.

Nuestra Asamblea Legislativa ha dado un pequeño paso hacia delante en la regulación de los derechos en el espacio cibernético. Se trata del proyecto de ley que intenta crear un Código Cibernético.[89] El proyecto intenta proteger el derecho a la intimidad que se ve más amenazado con la apertura que representa el mundo cibernético.[90] No obstante, el mismo se enfoca en proteger a la sociedad contra el acecho cibernético[91] y la pornografía[92]. El proyecto no ofrece protección contra los fragmentos de información que se van dejando en el Internet y la posibilidad de que los mismos sean recopilados por agentes privados o gubernamentales. Más aún, el proyecto de ley ha sido criticado por sus defectos y vaguedades.[93] Se ha contemplado que pueden surgir violaciones a la libertad de prensa y de expresión a raíz de la implementación del Código por ser éste demasiado abarcador.[94]

De ser aprobado como ley, el Código Cibernético garantiza ser un adelanto al derecho cibernético de nuestro ordenamiento, siguiendo la tendencia ya establecida en el ámbito federal. Sin embargo, al momento parece ser que el mismo traerá más fricciones constitucionales que una garantía a la intimidad en el Internet.

---

[89] Cyber Code of 2010, P. de la C. 2408, 16ta Asamblea Legislativa, 3ra Sesión Ordinaria (24 de enero de 2010).

[90] *Id*.

[91] Por su parte, el "cyberstalking" es llevar amenazas que causen considerable angustia emocional y/o física utilizando equipos electrónicos o cibernéticos. En el "internet" se configuran por constantes mensajes mediante correo electrónico, o cualquier página de interacción social.

[92] Asimismo, el "internet" se está convirtiendo aceleradamente en el mercado idóneo para los ofensores y delincuentes que buscan adquirir material para sus colecciones de pornografía infantil. Más insidioso que el intercambio de material de sexo explícito entre adultos, la pornografía infantil a menudo describe el asalto sexual de un niño y es a menudo utilizado por los pedófilos para reclutar, seducir y controlar a sus víctimas.

[93] En una entrevista, el Prof. Hiram Meléndez Juarbe expresó que lo que "logra es regular conducta que ya está atendida por otras leyes, y que en la mayoría de los casos, no requieren enmienda para que se extiendan al contexto digital". G. Ruiz Kuilan, *El Cyber Code en blanco y negro*, El Nuevo Día 30-31 (18 de abril de 2010).

[94] J. A. Delgado, *Levanta ampollas el "Cyber Code" cameral*, El Nuevo Día 20-21 (15 de abril de 2010).

V. La protección jurídica de la intimidad estadounidense y la española

En Estados Unidos se ha adoptado el análisis de expectativa razonable de intimidad cuando hay un reclamo de violación a la intimidad en Internet. En un caso relacionado a la obtención de números de teléfono, el Tribunal Supremo Federal resolvió que los usuarios de teléfono no contaban con una expectativa subjetiva de intimidad y por lo tanto, no estaban protegidos constitucionalmente.[95] El Tribunal fundamentó su decisión en el hecho de que los números telefónicos se conocían y que la compañía telefónica podía grabarlos para propósitos legítimos del negocio.[96] Por analogía, se desprende entonces que los correos electrónicos no gozan de una expectativa razonable de intimidad ya que los I.S.P.s los monitorean ordinariamente para asegurarse que no contengan pornografía infantil o virus.[97]

Bajo *Smith*, podríamos concluir que la información provista a un motor de búsqueda no goza de una expectativa razonable de intimidad, ya que la misma se le está proveyendo a un tercero (como, por ejemplo, Google). En otras palabras, al entrar las palabras claves en el motor de búsqueda asumimos el riesgo de que la información pueda ser utilizada por el motor de búsqueda para otros propósitos.

Aquí cabe hablar de un defecto que tienen las doctrinas de *Katz*, *Miller* y *Smith,* en el sentido que relacionan la protección constitucional con la expectativa de intimidad. Parece lógico razonar que cuando gozamos de una expectativa de intimidad, vamos a tener mayor protección constitucional. De igual forma, si no tenemos esa expectativa, no aplica la garantía constitucional. Pero este análisis tiene un defecto, y es que se basa estrictamente en la *expectativa*. Es decir, si de antemano el Gobierno anuncia que va a monitorear todas nuestras comunicaciones en el Internet, pues automáticamente no gozaríamos de una expectativa de intimidad, y no aplicaría la Cuarta Enmienda.[98] Consecuentemente, la mera sospecha o duda de que el gobierno monitoree lo que buscamos en Internet sirve para privarnos de toda protección constitucional. Un motor de búsqueda que prometa no compartir la información recopilada con terceros, brindaría a sus usuarios una expectativa de intimidad.

La doctrina de asunción de riesgo va atada a una noción de estar en libertad de escoger si uno desea asumir el riesgo o no. Pero muchas personas, cuya vida diaria o profesión se lo exige, no gozan de esa libertad de escoger si asumen el riesgo o no. Si no tienen la libertad de no revelar esa información a terceros, automáticamente se exponen a ser vigilados por el gobierno. Por lo tanto, la doctrina de asunción de riesgo es defectuosa porque muchas veces los usuarios revelan información personal en el Internet, no porque así quieren o porque no gozan de expectativa de intimidad

---

[95] *Smith v. Maryland*, 442 U.S. 735 (1979).

[96] *Id*. en la pág. 743.

[97] Tokson, *supra* n. 23, en la pág. 2158.

[98] *Smith*, 442 U.S. en la pág. 740.

alguna, pero porque no tienen opción; su profesión o las circunstancias se lo requieren. En realidad la única opción que tienen los usuarios al decidir si revelan información es usar los motores de búsqueda conscientes de que pierden toda expectativa de intimidad, o revertir a otra era y no aprovecharse de los adelantos tecnológicos.

En España, el enfoque que se le ha dado a controversias del derecho a la intimidad en Internet ha sido contrario al que se le ha dado en Estados Unidos. En vez de enfocarse en encontrar una expectativa razonable de intimidad antes de conceder la protección, se han concentrado en hacer valer el derecho a la intimidad, partiendo de la premisa de que "la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad".[99] Las sentencias emitidas por el Tribunal Constitucional Español desde el 1993 hasta el presente han ido estableciendo que el derecho a la protección de datos personales es uno fundamental y que todo ciudadano tiene derecho a exigir la protección de sus datos. En específico, la STC 292/2000, que aborda el tema de la transferencia de datos personales entre Administraciones Públicas sin el consentimiento de los afectados, consagró el derecho a la protección de datos de carácter personal como un derecho fundamental independiente, desvinculado del derecho a la intimidad.

VI. El futuro esquema legal de Puerto Rico

Ante una controversia de información recopilada a través del Internet, existen varias posturas que un tribunal podría tomar para resolverla. Tomando como modelo la doctrina federal, hay cuatro posibles alternativas para los tribunales. En primer lugar, el tribunal podría determinar que el contenido de la información que proviene de correos electrónicos y de navegar el Internet está protegido bajo la expectativa razonable de intimidad y que la doctrina de asunción de riesgo, cuando la información está en manos de terceros, se limita a información de no contenido. Bajo esta postura, al determinar si la información es de contenido, se resuelve si hay una expectativa de intimidad. En segundo lugar, el tribunal puede aplicar la doctrina de *Smith,* de información en manos de terceros, y distinguir entre el contenido de la información y los números de teléfonos. En tercer lugar, el tribunal puede resolver que toda la información recopilada en Internet se le revela a un tercero y por lo tanto, los usuarios no gozan de una expectativa de intimidad. Por último, el tribunal podría acoger la postura que la información de Internet no es de contenido y por lo tanto, no le aplica la protección de la Cuarta Enmienda.

De optar por seguir el marco jurídico español, nuestro Tribunal Supremo podría desarrollar la protección de datos personales como una vertiente del derecho a la intimidad. No obstante, lograr el desarrollo de un derecho de rango constitucional a la protección de datos, requiere una enmienda a nuestra Constitución o a la

[99] S.T.C. 11/1998 de 13 de enero.

Constitución Federal; lamentablemente, el uso de la informática aún no ha sido plasmado en nuestra Constitución.

Por tal razón, aunque nuestro derecho a la intimidad es de alta jerarquía, el Tribunal Supremo no ha demostrado la tendencia a favorecerlo sobre una intromisión en la comunicación. De surgir una controversia en un tribunal entre una violación al derecho de la intimidad frente a un posible atentado a la seguridad o a un interés sustancial del Estado, el interés del Estado debería prevalecer sobre el derecho a la intimidad. Sin embargo, si se opone el derecho a la intimidad frente al de una entidad privada que utiliza la información para fines de publicidad y mercadeo, una vez evaluada la expectativa de intimidad, hay una mayor posibilidad de que prevalezca el derecho a la intimidad. Por último, si la controversia que surge gira en torno a si una entidad gubernamental le puede exigir a una entidad privada la información recopilada, se debería analizar el contenido de la información solicitada para determinar si se gozaba de una expectativa de intimidad sobre la misma.

Con miras a garantizar la mayor protección del derecho a la intimidad en un área de Derecho donde la tecnología evoluciona constantemente, nuestra legislatura debería iniciar la aprobación de un esquema legal apropiado para el área del Derecho Cibernético. Lo fundamental al elaborar un esquema legal apropiado para el uso del Internet, es basar el mismo en las leyes actuales que rigen la propiedad, las transacciones comerciales y los daños para poder integrar el Internet a un contexto más amplio y general.[100] Empezar a elaborar un esquema tomando como base exclusivamente al Internet sería ineficiente, ya que se perderían las nociones generales que rigen nuestro ordenamiento.

Al momento, ni la jurisdicción federal ni la puertorriqueña cuentan con un esquema coherente y cohesivo para regir el ámbito de las comunicaciones a través de computadoras y el Internet. Lo poco que hay se desprende de interpretaciones que se han hecho de leyes que aplicaban a otro tipo de tecnología, así como disposiciones que garantizan derechos constitucionales. El análisis jurisprudencial anteriormente realizado revela que es una tarea imposible desarrollar un esquema que se pueda adaptar a cada tecnología en particular porque la realidad es que la tecnología evoluciona a un paso más rápido que el Derecho.

Por lo tanto, el esquema legal a desarrollarse no debe enfocarse en la tecnología particular (ya sea Internet, teléfono móvil o radio), sino más bien en la información en controversia. En otras palabras, sería impráctico desarrollar un esquema legal en términos de la tecnología empleada porque el mismo sería específico a cada caso particular y, lo que aplique para un caso, no necesariamente aplicaría para otro. Sería más útil elaborar un sistema en términos de la información que se recopila, que se guarda y que se revela a otras partes.[101] Este enfoque concuerda con el método

---

[100] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. Legal F. 207. ("The best way to learn the law applicable to specialized endeavors is to study general rules.")

[101] Jacqueline Lipton, *A Framework for Information and Law Policy*, 82 Or. L. Rev. 695, 702 (2003).

español de proteger todos los datos personales, irrespectivamente de dónde se publiquen.

Tiene sentido enfocar el esquema en la información, ya que la mayoría de las controversias que surgen sobre el Internet involucran la diseminación y el control de información recopilada.[102] Se le debe ofrecer protección al tipo de información, que es lo que la sociedad verdaderamente valora, en vez de enfocarse en la tecnología a través de la cual se guarda información y posteriormente se comunica.[103] El esquema legal a desarrollarse debe tomar en cuenta un esquema bipartita para lograr una efectiva protección constitucional. En primer lugar, se hace un balance entre el derecho a acceder información y el derecho a revelar la información. En segundo lugar, se evalúa si existe una expectativa razonable de intimidad, subjetiva y objetivamente.

A. Un balance entre derechos

Se ha sugerido que luego de enfocar el esquema legal en la información, se elabore un "rights-based model" o esquema basado en los derechos protegidos.[104] Estoy de acuerdo con esta propuesta ya que los derechos que una parte tenga a la recopilación de información o a su posterior revelación son casi siempre la esencia de toda controversia jurídica en este ámbito. Los derechos que se concedan deben organizarse en los que garantizan la intimidad en cuanto a cierta información y aquellos que brindan acceso a la información. El esquema tendría como objetivo lograr un balance entre el acceso a la información, que a su vez incluye la facultad de aprovechar la tecnología, y la intimidad de las personas en cuanto a la información accedida. La principal ventaja que tiene este esquema es que no tiene como base unos conceptos radicales ni poco familiares. Por el contrario, la idea de hacer un balance de intereses entre el derecho de acceso a la información y el derecho a controlar la información que se accede nos parece muy familiar. [105]

Por tratarse de un balance entre derechos, habrá ocasiones en que el derecho a acceso de información irá por encima del derecho a la intimidad sobre la información. Estas instancias se pueden tomar en consideración al desarrollar el esquema. Por ejemplo, cuando se trata de información sobre la cual el gobierno tiene

---

[102] *Id*. en la pág. 704.

[103] Dane McLeod, *Regulating Damage on the Internet: A Tortious Approach?*, 27 Monash U. L. Rev. 344, 350 (2001).

[104] Lipton, *supra* n. 97, en la pág. 706.

[105] Un escrutinio de balance de intereses entre derechos parece ser cónsono con lo que varios tribunales federales han resuelto al tener que sopesar el derecho a la intimidad con la libertad de expresión. *Véase* Cecilia M. Suau Badía, Autor Estudiante, *El Anónimo y el Seudónimo, Piedras Angulares de la Libertad de Expresión en el Internet*, 43 Rev. Jurídica U. Inter. P.R 551, 666 (2009); *E.L.A. v. Hermandad de Empleados del Negociado de Seguridad de Empleos y Otros*, 104 D.P.R. 436 (1975); *Fulana de Tal v. Demandado*, 138 D.P.R. 610 (1995).

un interés sustancial en accederla, ya sea para evitar terrorismo o para mantener la seguridad, el derecho a acceso del gobierno puede ir por encima del derecho de intimidad de la persona. Por el contrario, si se trata de una persona que está accediendo la información de manera ilegal (*hacking*), entonces el derecho a la intimidad prevalecerá. Los derechos que se balancearán consisten en aquellos de acceso y los de control o intimidad.

i. El derecho a acceder información

El derecho a acceder información implica una autorización previa o permiso para acceder la información. Pero de mayor importancia que la autorización para acceder la información, es el propósito para el cual se accede. Información que se utiliza para iniciar un proceso judicial, por ejemplo, viene acompañada de un propósito que adelanta la política pública. Por lo tanto, dicha información tiene más probabilidad de ser accedida y, de ser necesario, sería posible obtener una orden judicial para accederla.

No obstante, la mayoría de la información personal que se recopila por agencias privadas se usa para efectos de publicidad. Cabe hablar aquí del controversial caso de DoubleClick, una compañía que se dedica a recopilar información de los usuarios de Internet para dirigirles anuncios en el Internet.[106] DoubleClick recopila la información a través de *cookies* y actúa como intermediario entre las páginas web que navegan los usuarios y las compañías que desean anunciarse en Internet. La Corte de Distrito resolvió a favor de la práctica de DoubleClick al entender que su método de identificación vía *cookies* era interno en la compañía y exclusivamente para la misma. Sólo si DoubleClick hubiese actuado con un propósito torticero hubiera tenido que responder en daños.[107]

El caso de DoubleClick demuestra la renuencia de los tribunales a negar el derecho de acceso a información a las compañías privadas. Parece indicar que se utilizará el subterfugio de "propósito interno" para cada controversia de acceso a información. Por eso, es indispensable que el derecho a acceder información no se analice exclusivamente y que, al contrario, se sopese con el derecho a revelar información personal que tienen los usuarios.

ii. El derecho a controlar información

El derecho a controlar el acceso a la información tiene como base el derecho a la intimidad pero, a su vez, se distingue del derecho de propiedad en que se utiliza exclusivamente para proteger la autonomía de la persona.[108] Su esencia recae en el

---

[106] *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[107] Ku & Lipton, *supra* n. 15, en las págs. 660-661.

[108] Un derecho de propiedad puede ser utilizado en un ámbito comercial para proteger patentes o "trade secrets". *Véase* Jessica Litman, *Information Privacy/Information Property*, 52 Stan. L. Rev. 1283, 1284 (2000).

reclamo de una persona para controlar la diseminación, uso o acceso a información pertinente a esa persona; se enfoca en el individuo y su información personal.[109] En nuestro ordenamiento, el derecho a controlar la información que se accede debería ser de una jerarquía superior al de acceder información debido a que la intimidad tiene un gran valor. No obstante, al igual que el derecho a la intimidad, el mismo no sería absoluto y cedería ante el Estado, de existir un interés apremiante.

Además de estar ligado a la intimidad, el derecho a controlar el acceso depende del tipo de información que se intente acceder. Por ejemplo, si lo que se busca acceder es información personal, como perfiles de clientes, historiales de compra o récords financieros, el derecho a controlar dicha información será mayor. Incluso, el derecho sobre la información personal es tan importante que la información personal puede ser una categoría de por sí, equivalente a un derecho de propiedad. De ser así, la extracción y diseminación de dicha información puede ser limitada por medidas tecnológicas de protección.

B. La expectativa de intimidad

Como segundo paso, se debe tomar en cuenta la expectativa de intimidad de aquella persona cuya información se accede. Se debe emplear un análisis objetivo y subjetivo, según discutido anteriormente, para determinar si la persona alberga una expectativa de intimidad sobre la información. Además, se debe evaluar si la sociedad entiende que el usuario tiene una expectativa de intimidad socialmente razonable sobre esa información.[110]

Hay ocasiones en que se desprende de un contrato en el cual una parte garantiza confidencialidad; ahí se podría fácilmente concluir que hay una expectativa de intimidad. No obstante, en situaciones donde no hay un contrato entre las partes, los legisladores deben tomarse la tarea de determinar si las partes gozan de una expectativa de intimidad. Dependiendo de la expectativa de intimidad que se determine, se ofrecerá protección contra el acceso sin autorización. Como excepción, se puede aplicar un escrutinio judicial especial para los casos en que se presente una medida tecnológica con un impacto sobre la intimidad mayor al necesario, independientemente de si hay una expectativa a la intimidad.[111]

VII. Conclusión y recomendación

La necesidad de un sistema legal que regule el Internet es una realidad que ha cobrado vigencia en las últimas décadas. La evolución del Internet y nuestra

---

[109] Lipton, *supra* n. 97, en la pág. 737.

[110] Aunque personalmente discrepo con el uso del escrutinio de la expectativa razonable de intimidad por encontrarlo defectuoso, entiendo que es indispensable que el mismo se incorpore al esquema legal, ya que es la tendencia tanto en la jurisdicción federal como en la puertorriqueña cuando se enfrenta a una controversia de derecho a la intimidad.

[111] Meléndez Juarbe, *supra* n. 37, en la pág. 76.

interacción con el mismo ha evolucionado tan drásticamente que las leyes que regulaban las telecomunicaciones se han tornado anticuadas e inaplicables. Por tal razón, la creación de un esquema legal que se enfoque en preservar nuestro derecho a la intimidad es esencial. A pesar de que recientemente nuestra Asamblea Legislativa se ha dado la tarea de crear un Código Cibernético, el mismo no regula la información personal que los usuarios de Internet van dejando en el mundo cibernético y que puede ser recopilada por agencias privadas y gubernamentales.

La razón principal por la cual carecemos de protección constitucional en el Internet es porque el esquema legal presente se concentra en la tecnología o el medio a través del cual se expone o recopila la información. Por eso, es indispensable que el nuevo esquema legal a crearse se enfoque en el tipo de información que se hace disponible, tomando en consideración si estamos conscientes de que la estamos exponiendo y permitimos revelarla y si el que la recopila lo hace para un propósito legítimo. Este esquema se puede aplicar a compañías privadas, así como a entes gubernamentales para intentar que prevalezca el derecho a la intimidad.

El Internet juega un rol demasiado amplio en el mundo contemporáneo para que el uso del mismo carezca de protección constitucional. No se sabe cómo nuestros tribunales se expresarán ante una controversia del derecho a la intimidad en el Internet. No obstante, espero que el presente trabajo de investigación sirva de guía, ya que recoge la doctrina federal, la española y la puertorriqueña para el esquema legal que se debe desarrollar, así como la postura que pudiesen adoptar los tribunales en un futuro cercano.