LOS REGISTROS Y ALLANAMIENTOS EN LA ERA DIGITAL: LA RENUNCIA A NUESTRA PRIVACIDAD

ARTÍCULO

Julia Inés Reyes

I. Introducción

Los avances tecnológicos han minado de retos a nuestro ordenamiento jurídico en término de las salvaguardas constitucionales que consagran nuestro derecho a la intimidad y la obtención de información personal por parte del Estado. Es decir, a medida que las innovaciones tecnológicas se han hecho más accesibles a la población, el intercambio de información se ha facilitado, y por ende, ha surgido un incremento en el riesgo de que terceros tengan acceso inmediato a determinada información personal.

Bien es sabido, que el surgimiento de nuevos sistemas de comunicación se ha caracterizado por la unificación global de las naciones, lo que ha moldeado el comportamiento social, económico y político de los países que ostentan acceso a diversos avances tecnológicos.[1] Así, esta transformación ha creado nuevas formas de intercambio de información, lo que ha provocado nuevos retos en cuanto al derecho de libertad de expresión, el desarrollo de la informática y el rol de la población en esta creciente modalidad.[2] Asimismo, en el ámbito jurídico, ha provocado un sinnúmero

---

* Estudiante de cuarto año de la Facultad de Derecho de la Universidad Interamericana de Puerto Rico. La autora tiene un bachillerato en Administración de Empresas, con concentración en Comercio Internacional de la Universidad de Puerto Rico, Recinto de Humacao. Asimismo, cursó una maestría en Relaciones Internacionales con un enfoque en Resolución de Conflictos en Northeastern University de Boston, Massachusetts. Agradezco al Hon. Julio De la Rosa Rivé, cuyas observaciones, sugerencias y críticas contribuyeron a la investigación y desarrollo del presente artículo jurídico. Por último, agradezco a mi familia por ser mi soporte incondicional.

[1] Manuel Castells, *The Rise of the Network Society,* Vol. I, 357 (2d ed., Wiley-Blackwell 2000).

[2] UNESCO, *Global Media and Information Literacy Assessment Framework: Country Readiness and Competencies* 9 (UNESCO 2013).

de dilemas entre la dicotomía de protección del derecho a la intimidad y el acceso de los Estados a obtener información personal de la población para mantener la seguridad de la población.

A medida que se han ido desarrollando avances tecnológicos e instrumentos de acceso a la informática, tanto los tribunales de Estados Unidos como los de Puerto Rico han incorporado ciertas doctrinas jurisprudenciales que pretenden estandarizar la expectativa de intimidad de la población y los mecanismos, de los que goza el Estado, para poder tener acceso a la información. Por tal motivo, la materia de registros y allanamientos ostenta un rol crucial, toda vez que, a medida que la tecnología se encuentra en un creciente desarrollo, se han suscitado controversias en torno a la aplicabilidad de la Cuarta Enmienda de los Estados Unidos y su interpretación por la Corte Suprema Federal.[3]

En atención a ello, este escrito realiza un análisis en materia de registros y allanamientos frente al continuo desarrollo tecnológico. Es decir, evaluaremos la utilización de tecnología como instrumentos de almacenaje de información, comunicaciones y redes sociales. De igual forma, evaluaremos la intervención del Estado para obtener información tanto de instrumentos tecnológicos como de las redes del internet. Así pues, discutiremos el balance de poder del Estado y el derecho a la intimidad de los individuos frente a los avances tecnológicos y el intercambio libre de información personal tanto en forma de *metadata* como de contenido. Veremos además, si existe una tendencia a que el Estado expanda su poder ante los cambios tecnológicos, o por el contrario, restringa su poder ante las innovaciones tecnológicas.

Por tanto, surgen ciertas interrogantes respecto a si uno renuncia a su derecho a la intimidad o privacidad una vez acceda las redes de la informática, cuando utiliza su correo electrónico, sus cuentas de redes sociales o comparta información privilegiada con su entidad financiera o en los servicios de búsqueda en la red. Por otro lado, emerge la prerrogativa de la doctrina de registros y allanamientos y su propósito de preservar el derecho a la intimidad de los individuos y evitar registros ilegales e irrazonables.

Preciso es puntualizar, que en el caso *United States v. Jones*, la Jueza Sonia Sotomayor, en su opinión concurrente, plantea que sería "necesario reconsiderar la premisa de que un individuo no posee una expectativa razonable de intimidad en información ofrecida a un tercero . . . [e]ste análisis no guarda concordancia con la era digital, en la que las personas revelan una vasta cantidad de información personal a terceros en actividades de la vida diaria".[4] (Traducción nuestra).

---

[3] La Cuarta Enmienda de La Constitución de Estados Unidos establece que "[n]o se violará el derecho del pueblo a la seguridad de sus personas, hogares, documentos y pertenencias, contra registros, detenciones o incautaciones irrazonables, y no se expedirá ningún mandamiento sino en virtud de causa probable, apoyado en juramento o afirmación, que describa particularmente el lugar que ha de ser registrado, y las personas o cosas que han de ser detenidas o incautadas." (Énfasis y traducción nuestra).

[4] *United States v. Jones*, 132 S. Ct. 945, 957 (2012).

Así las cosas, este escrito expone la trascendencia de la jurisprudencia federal y puertorriqueña, en un intento de atemperar el ordenamiento jurídico a las nuevas corrientes de intercambio de información por medio de instrumentos tecnológicos.

II. Registros y allanamientos

A. El efecto de los avances tecnológicos en la jurisprudencia sobre la Cuarta Enmienda de los Estados Unidos.

La Cuarta Enmienda de los Estados Unidos dispone, a saber: que no se violará el derecho del pueblo a la seguridad de las personas, hogares, documentos y pertenencias, contra registros, detenciones e incautaciones irrazonables, y no se expedirá ningún mandamiento sino en virtud de causa probable, apoyado en juramento o afirmación, que describa particularmente el lugar que ha de ser registrado, y las personas o cosas que han de ser detenidas o incautadas.[5] La Cuarta Enmienda es ápice constitucional para la protección de todo tipo de detención personal, registros o allanamientos de efectos personales o propiedad o lugar en el que un individuo ostente expectativa de intimidad.[6] Lo anterior significa que la protección de la Cuarta Enmienda se extiende específicamente a aquellas actuaciones irrazonables por parte del ente gubernamental. Por tal motivo, para evitar cualquier ilegalidad o actuación irrazonable por parte del gobierno en el proceso de registro y allanamiento, la Cuarta Enmienda añade el criterio de la orden o *warrant.* Ello pretende, pues, entablar un balance entre el interés del individuo registrado y el poder ejecutivo, toda vez que, el primero no quiere que nada sea registrado y el segundo tiene como norte lograr una convicción.[7] Por cuanto, la prohibición de la Cuarta Enmienda en contra de registros y allanamientos irrazonables pretende mantener un balance entre intereses paradójicos, a saber: (1) el derecho de un individuo a su privacidad y (2) el derecho de la sociedad a la seguridad y lograr la convicción de aquellos que delinquen.[8]

Las disposiciones de la Cuarta Enmienda surgieron en Estados Unidos como respuesta a las experiencias durante la era inglesa y colonial, en las que existían las órdenes generales o mandamientos.[9] Estas órdenes y mandamientos generales facultaban a los oficiales del rey a entrar en casas privadas y registrar las propiedades para encontrar cualquier tipo de material delictivo.[10] Lo anterior, sin esbozar especificidad alguna sobre el material o lugar a ser registrado o allanado.[11] Por

---

[5] U.S. Const. Amend. IV.
[6] Ernesto L. Chiesa Aponte, *Derecho Procesal Penal de Puerto Rico y Estados Unidos,* Vol. I, 181 (Editorial Forum, 1995).
[7] *Id.*
[8] L. Anita Richardson, *Why the Fourth Amendment Doesn't Stand Still,* 26 No. 3 Judges' J. 48 (Summer 1987).
[9] Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L. Rev. 531, 536 (2005).
[10] *Id.*
[11] *Id.*

tal motivo, la Cuarta Enmienda se creó con el objetivo principal de garantizar que el gobierno federal no ostentara poderes ilimitados en materia de registros y allanamientos. Es decir, se prohíben las órdenes generales y se establece el criterio de la razonabilidad y el requisito de incluir en la orden el lugar exacto a ser registrado y la persona o cosa a ser allanada.[12] Asimismo, se incluyó el principio de la razonabilidad, el cual es utilizado por el Tribunal para mantener un balance de intereses entre la necesidad de intromisión por parte del Estado para mantener la seguridad y entre aquellos intereses particulares de cada individuo.[13]

Cónsono con lo anterior, las disposiciones de la Cuarta Enmienda, por lo general, son percibidas como registros de las casas y por ende una invasión a las expectativas de intimidad de los propietarios, salvo que sea subsanado por la obtención de una orden o mandamiento judicial, o en la alternativa, que apliquen algunas de las excepciones a la norma.[14] En atención a ello, en el año 1967 el Tribunal Supremo de Estados Unidos (en adelante, T.S.E.U.), resuelve el caso de *Katz v. United States*,[15] el cual, por medio de la opinión concurrente del Juez Harlan, estableció un estándar de prueba, mejor conocido como el *test* de *Katz*. En este caso, al acusado se le imputaba haber transmitido información sobre apuestas por vía telefónica de Los Ángeles a Miami y a Boston, en contravención de las disposiciones de un estatuto federal. En vista de ello, el acusado solicitó la supresión de la conversación telefónica, obtenida por agentes del *Federal Bureau of Investigation* (en adelante, FBI), toda vez que, fue obtenida mediante el uso de instrumentos electrónicos colocados en la cabina telefónica para obtener las grabaciones de las conversaciones. A tales efectos, el Tribunal de Apelaciones mantuvo la convicción del acusado bajo la tesis de que la Cuarta Enmienda, no era de aplicación al caso porque no se efectuó una intromisión física al área en la cual se encontraba el acusado.

Sin embargo, el T.S.E.U. estableció que en los casos en los cuales el Estado escuche y grabe, por medio de la utilización de aparatos electrónicos, las conversaciones de individuos que usan cabinas de teléfonos públicos, ciertamente contraviene las protecciones de la Cuarta Enmienda.[16] Lo anterior significa que la actuación del Estado configura un registro y allanamiento cobijado por la Cuarta Enmienda y que la doctrina ha de extenderse a la protección de los individuos y no únicamente a los lugares. El Tribunal estableció, a saber:

> [L]a Cuarta Enmienda protege a las personas, no los lugares. Lo que una persona a sabiendas expone al público, aunque sea en su propia casa u oficina, no está sujeto a la protección de la Cuarta Enmienda. Sin embargo, si actúa

---

[12] *Id.*

[13] William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment,* 44 Stan. L. Rev. 553, 562 (1992).

[14] *Kyllo v. United States*, 533 U.S. 27, 32-33 (2001).

[15] *Katz v. United States,* 389 U.S. 347, 361 (1967) (Harlan, J., concurrente).

[16] *Id.* pág. 353.

> de manera que busque preservar la privacidad, aunque el área esté accesible al público, podría ser constitucionalmente protegido.[17]

En este caso, el Estado arguyó que la vigilancia realizada no violaba las disposiciones de la Cuarta Enmienda debido a que la grabadora se encontraba en el área exterior de la cabina telefónica y que, por tal motivo, no afectaba el área que constitucionalmente sí estaba protegida.[18] Por el contrario, en *Katz*, el Tribunal arguyó que el Estado actuó en contravención a la Cuarta Enmienda, toda vez que violó su derecho a la intimidad. En virtud de ello, el T.S.E.U. rechazó ambos argumentos y estableció:

> En primer lugar la solución adecuada para los problemas relacionados a la Cuarta Enmienda no necesariamente están enmarcados en la frase "área constitucionalmente protegida". Segundo, la Cuarta Enmienda no puede ser traducida solo a la generalidad del derecho a la intimidad. Esta Enmienda protege la privacidad del individuo contra ciertos tipos de intromisiones del gobierno, pero su protección va más allá, y en muchas ocasiones no tiene nada que ver con la privacidad.[19]

Consecuentemente, el principio de **expectativa razonable de intimidad** comienza a jugar un rol trascendental, en términos de la aplicabilidad de la Cuarta Enmienda en casos en los que se arguya intromisión gubernamental. Por tal motivo, se estableció que las garantías de la Cuarta Enmienda serían aplicadas en ciertas instancias, a saber: (1) si las actuaciones del individuo denotan tener expectativa de intimidad; y (2) la expectativa de intimidad sea una generalmente reconocida por la sociedad.[20] Es menester destacar, que este caso introduce la expectativa o la razonabilidad de privacidad de acuerdo a las consideraciones del espectro colectivo. Así las cosas, es preciso comenzar a interpretar el desarrollo tecnológico cónsono con la accesibilidad de instrumentos tecnológico para la población.

A modo de ilustración, el caso de *Katz*, extiende la protección sobre expectativa razonable de intimidad a las grabaciones de teléfonos públicos, toda vez que, para la década de los sesenta la utilización de teléfonos públicos se convirtió en un mecanismo esencial y corriente para la población entablar conversaciones privadas. Podríamos colegir entonces, que según incrementa el número de instrumentos tecnológicos a los que la sociedad tenga fácil acceso, a tenor con el estándar de *Katz,* mayor será la

---

[17] *Id.* a la pág. 351, Traducción nuestra.

[18] *Id.* pág. 352. El Estado intenta argumentar que debido a que la grabadora fue colocada en el área externa de la cabina telefónica no se violaron los derechos del acusado bajo el palio de la Cuarta Enmienda.

[19] *Id.* pág. 350. Traducción nuestra.

[20] Samantha Arrington, *Expansion of the Katz Reasonable Expectation of Privacy Test Is Necessary to Perpetuate a Majoritarian View of the Reasonable Expectation of Privacy in Electronic Communications to Third Parties* 90 U. Det. Mercy L. Rev. 179, 182-183 (2013).

expectativa de intimidad sobre la tecnología que utilizamos para realizar actividades cotidianas, como el uso de comunicaciones electrónicas, información del Proveedor de Servicios de Internet, transacciones en la red de entidades financieras, y la utilización de redes sociales.

Es por tal motivo, que en el caso de *Katz*, el T.S.E.U. incluyó una nueva perspectiva en cuanto a la tecnología al establecer que:

> Una persona en una cabina telefónica puede confiar en la protección de la Cuarta Enmienda. Aquel que ocupa [la cabina], cierra la puerta y paga para poder realizar una llamada ciertamente puede asumir que las palabras que profiere a través del teléfono no serán difundidas al mundo. El interpretar la Constitución de forma estrecha es ignorar el rol vital que los teléfonos públicos han venido jugar en las comunicaciones privadas.[21]

Por otra parte, el T.S.E.U. no le ha asignado una definición precisa al término *razonabilidad* en el contexto de expectativa de intimidad, por consiguiente, adopta criterios sociales normativos y mayoritarios.[22] Lo anterior se refiere a que el Tribunal, recurre al manejo de instrumentos empíricos que reflejen la opinión mayoritaria de las masas o de un considerable porcentaje de la población. Así, ausculta lo que un puñado de la población considera como una expectativa razonable de la intimidad. No obstante, según ilustra la jurisprudencia norteamericana, los Tribunales implícitamente continúan aplicando los criterios normativos en materia de registros y allanamientos.[23] Si aceptamos para propósitos de argumentación el razonamiento del Juez Black en el caso de *Katz*, acerca de que la Cuarta Enmienda protege únicamente las cosas tangibles y no las conversaciones de todas formas no le cobijaría la razón. Ello es así, debido a que nos desvirtuaríamos del propósito medular de la Cuarta Enmienda de proteger a la población de la intromisión indebida del Estado en asuntos en los cuales los individuos tengamos expectativa de intimidad.[24]

En el caso de *Smith v. Maryland,*[25] agentes del gobierno adscritos al *National Security Administration* (en adelante, NSA), le solicitaron a una compañía de teléfono que instalara un instrumento electrónico, mejor conocido como "pen register", para grabar los números telefónicos realizados desde el teléfono de la casa de Smith. La compañía solo reveló los números de teléfono marcados pero no el contenido de las comunicaciones sostenidas por Smith o si en efecto las llamadas lograron conectarse.[26]

---

[21] *Katz*, 389 U.S. págs. 516-517. Traducción nuestra.

[22] Arrington, *supra*, n. 20, pág. 183.

[23] *Id.* págs. 183-184.

[24] *Katz*, 389 U.S. pág. 365.

[25] *Smith v. Maryland*, 442 U.S. 735, 737 (1979).

[26] *Id.* pág. 741. *Véase además:* el *Pen Register Act.* En 1986, la *Electronic Communications Privacy Act (ECPA),* fue creada (Pub. L. No. 99-508, 100 Stat. 1848), sobre el proceso de adquirir una orden judicial ex parte por parte de la Rama Ejecutiva para obtener información por medio del uso de *Pen Register.* De acuerdo con 18 U.S.C. Sec. 3123(a)(1), "[the] courts shall enter an ex parte order

Consecuentemente, el acusado arguye que poseía una expectativa razonable de intimidad en cuanto a los números de teléfono a los cuales llamaba. Sin embargo, el T.S.E.U. rechazó el argumento de Smith al establecer que:

> Dudamos que las personas en general presuman que tienen una expectativa de intimidad sobre los números a los que llaman. Todos los usuarios de teléfono saben que deben transmitir números de teléfonos a las compañías proveedoras de servicios telefónicos, dado que es mediante los equipos de estas compañías que sus llamadas son procesadas. Todos los suscriptores reconocen que las compañías de teléfono tienen la facilidad para realizar records permanentes de las llamadas que realizan los usuarios, toda vez que, en las facturas mensuales se provee la lista de las llamadas realizadas a larga distancia. De hecho, "pen registers" y otros instrumentos similares son utilizados rutinariamente por las compañías telefónicas…[27]

Lo anterior significa que el T.S.E.U. impone un factor de asunción de riesgo ya que la información obtenida por terceros por parte de un individuo no está protegida constitucionalmente por la Cuarta Enmienda aunque haya sido suministrada bajo la presunción y seguridad de que la información sería utilizada para propósitos limitados, como por ejemplo, información bancaria ofrecida con el propósito único de realizar una transacción o gestión bancaria.[28] De forma tal que en el caso de *Smith*, el T.S.E.U. basó su análisis en que el acusado voluntariamente ofreció la información numérica o *metadata* a la compañía telefónica. Por tal motivo, el acusado asumió el riesgo de que la compañía telefónica proveyera información numérica a las autoridades gubernamentales.[29]

Por todo lo cual, si comparamos el principio doctrinal de *Katz*, con el principio de información otorgada a tercero, ciertamente surge una inconsistencia en relación con la utilización moderna de la tecnología y los intereses que pretende proteger la Cuarta Enmienda. Es decir, a medida que la tecnología se ha convertido en un instrumento fundamental para realizar actividades cotidianas, es inevitable compartir información personal con terceros, actividades que de otra forma se considerarían actos privados.[30] Esta disparidad puede darse no solo con la *metadata* sino también en casos donde se comparta contenido. Es decir, que el tipo de información que se comparte con terceros, puede contener datos numéricos en forma de *metadata* o podría extenderse a información en forma de contenido. Por ejemplo, el tratadista

---

authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."

[27] *Id.* pág. 742. (Traducción nuestra).

[28] Arrington, *supra* n. 20, págs. 185-186.

[29] *Smith*, 442 U.S. págs. 743-745.

[30] Lon A. Berk, *After Jones, The Deluge: The Fourth Amendment's Treatment of Information, Big Data and The Cloud*, 14 J. High Tech. L. 1, 30 (2014).

Berk, nos provee un ejemplo claro de computación en la nube o *cloud computing*, pues se trata de un servicio a través de internet en la que se crean archivos virtuales con contenido de información personal y documentos de cualquier clase.[31] Así pues, el servicio de *cloud computing* crea enormes bases de datos, por lo que cada vez son más los individuos y negocios que dependen de este servicio de almacenamiento de información personal o comercial. La interrogante estriba en que esta información que proveen los negocios e individuos se almacena por medio de un tercero que provee el servicio de mantenimiento y almacenaje de la información.[32] Así, cualquier información que entremos en la base de datos de nuestra tableta, *Smartphone,* computadora o calendario, realiza una sincronización donde toda la información consta en los aparatos electrónicos simultáneamente. Para ello, es imprescindible que se procesen los datos con la intervención de un tercero, en este caso, el proveedor de servicio *cloud computing,* quien tendrá acceso a información que el individuo o la compañía estimen como privado o confidencial. Consecuentemente, surge el aspecto crítico en materia de la Cuarta Enmienda, toda vez que, podríamos argüir que cuando una persona adquiere el servicio de alguno de estos proveedores, renuncia a su interés privativo sobre la información almacenada y estaría sujeta a ser registrada o allanada.[33]

En virtud de lo antes expuesto, ciertamente la jurisprudencia concerniente a la interpretación de la Cuarta Enmienda tiene su génesis en los valores tradicionales, en los cuales la tecnología no jugaba un rol en la vida cotidiana y no era un instrumento de productividad, economía e interconectividad entre los individuos y naciones. Por tal motivo, es imperativo identificar los principios de la Cuarta Enmienda y adaptarlos a los constantes desarrollos tecnológicos. En este particular, es imperante puntualizar que la información que ofrecemos a nuestra entidad financiera no es la misma que ofrecemos a un amigo. Así pues, surge una serie de niveles en cuanto a la expectativa de intimidad de los individuos que comparten información en las redes cibernéticas. Lo anterior significa, que para mantener un balance entre los intereses del Estado sobre las convicciones y el de los individuos sobre su expectativa de intimidad, es preciso catalogar la información protegida por la Enmienda y aquella que por la naturaleza explícita de su publicación no merece ser protegida de registros o allanamientos.

Las reacciones y críticas de la interpretación jurisprudencial de *Katz*, no se hicieron esperar, toda vez que, la protección de la Cuarta Enmienda pasó a tener una noción de privacidad a nivel individual.[34] Así las cosas, en los casos más recientes como *United States v. Jones,*[35] el T.S.E.U. se topó con la controversia sobre si colocar

---

[31] *Id.*

[32] Entre las plataformas más conocidas de *Cloud Computing* se encuentran iCloud, Dropbox, Google, Apps y SaaS. *Véase también* David Linthicum, *What's Driving Corporate Cloud Use? Home Cloud Use*, http://www.infoworld.com/d/cloud-computing/whats-driving-corporate-cloud-use-home-cloud-use-213490 (accedido 24 de octubre de 2014).

[33] Jed Rubenfeld, *The End of Privacy,* 61 Stan. L. Rev. 101, 107 (2008).

[34] Berk, *supra* n. 30, págs. 13-14.

[35] *U.S. v. Jones*, 132 S. Ct. 945 (2012).

un GPS o dispositivo de rastreo en el vehículo de un individuo y utilizar el artefacto para monitorear los movimientos del vehículo por las carreteras públicas, constituía un registro y allanamiento al amparo de la Cuarta Enmienda. En este caso al acusado se le imputaba haber conspirado para distribuir y poseer con intención de distribuir cinco (5) kilos o más de cocaína y cincuenta (50) gramos o más de base de cocaína en violación de las disposiciones, a saber: 21 U.S.C. § 841 y 21 U.S.C. § 846, por lo que fue sentenciado a prisión de por vida. Así las cosas, el Estado presentó como prueba información obtenida por mediodel GPS que anteriormente había sido suprimida y en el que se radicaron los mismos cargos. La referida información, vinculaba al acusado con los delitos que se le imputaban. Cabe mencionar que el Estado tramitó una orden judicial que le permitía colocar el dispositivo GPS en el vehículo de la esposa del acusado.[36] La orden autorizaba a que se instalara el artefacto en el vehículo dentro de diez (10) días y que fuera en el Distrito de Columbia.[37]

El Estado rastreó el vehículo por veintiocho (28) días, manteniendo constancia de los lugares a donde se dirigía. Por tal motivo, el T.S.E.U. estableció que la instalación del dispositivo de rastreo en el vehículo y el monitoreo constante de la ubicación del mismo, conformaba un registro.[38] Este caso cobra vital importancia pues la opinión mayoritaria por voz del Juez Scalia, retoma el examen sobre ocupación física en propiedad ajena. Es decir, el Juez Scalia retoma el análisis a base de la intromisión física por parte del Estado en propiedad privada para obtener información, alejándose así de jurisprudencia de años recientes sobre la expectativa de intimidad.[39] Sin embargo, es preciso hacer mención de las opiniones concurrentes de la Jueza Sotomayor y el Juez Alito, las cuales reconocen el exponencial desarrollo de la tecnología, que cada vez está más accesible a la población en general.[40] Así pues, realizan un llamado a reconsiderar la expectativa de intimidad de los individuos ante la era digital en la que la tecnología que utilizamos a diario es tan avanzada que con un simple toque podemos conocer la localización de otros y demás datos personales. A su vez, debemos precisar que la doctrina de ocupación física podría verse en detrimento, toda vez que la tecnología inalámbrica permite rastrear, monitorear o conocer detalles de las personas desde lugares remotos. Por tanto, es menester realizar un examen sobre qué expectativa de intimidad tenía el individuo en ese preciso momento.

Al mismo tiempo, la Jueza Sotomayor plantea que es preciso reconsiderar la doctrina de asunción de riesgo al compartir información con terceros, debido a que no guarda correlación con la era digital debido a que hoy día la mayor parte de las personas se ven forzadas a compartir información con terceros para poder cumplir con las obligaciones cotidianas. Así pues, añade:

---

[36] *Id.* pág. 948.
[37] *Id.*
[38] *Id.* pág. 949.
[39] *Id.*
[40] *Id*. págs. 954-964.

> I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[41]

B. Los registros y allanamientos en Puerto Rico ante la Era digital

La protección de la Cuarta Enmienda federal se extendió en su totalidad a Puerto Rico.[42] Además, el T.S.E.U. estableció que el requisito de causa probable para registros, allanamientos y arrestos por autoridad judicial, según dispone la Cuarta Enmienda aplica a Puerto Rico.[43] Por su parte, la sección 10 del artículo II de la Constitución de Puerto Rico dispone que "no se violará el derecho del pueblo a la protección de sus personas, casas, papeles y efectos contra registros, incautaciones y allanamientos irrazonables".[44] Asimismo, establece que "solo se expedirán mandamientos autorizando registros, allanamientos o arrestos por autoridad judicial y ello únicamente cuando exista causa probable apoyada en juramento o afirmación, describiendo particularmente el lugar a registrarse y las personas a detenerse o las cosas a ocuparse. Evidencia obtenida en violación de esta sección será inadmisible en los tribunales".[45]

Bien es sabido que en reiteradas ocasiones, el Tribunal Supremo de Puerto Rico (en adelante, T.S.P.R.) ha puntualizado que el objetivo principal de la disposición constitucional es proteger la intimidad y dignidad de las personas, así como de las pertenencias, domicilio o propiedad frente a las actuaciones arbitrarias e irrazonables por parte del Estado.[46] Esta protección constitucional cobra vigencia si la persona que la invoca ostenta el derecho a una expectativa razonable a la intimidad sobre el lugar o las cosas registradas, por lo que hay ciertas instancias en las que no es necesario tener una orden judicial para que un agente del orden público proceda a registrar e incautar evidencia.[47] No obstante, los registros y allanamientos que se efectúen basados en una orden judicial gozan de una presunción de legalidad y razonabilidad.[48] Consecuentemente, el esquema establecido en la Constitución de

---

[41] *Id.* pág. 957.
[42] *Torres v. Puerto Rico*, 442 U.S. 465, 471 (1979).
[43] Dora Neváres-Muñíz, *Sumario de Derecho Procesal Penal Puertorriqueño* (9na ed., Instituto para el Desarrollo del Derecho, Inc. 2011).
[44] Const. P.R. art. II, § 10.
[45] Const. P.R. art. II, §10.
[46] *Pueblo v. Ferreira Morales*, 147 D.P.R. 238, 249 (1998).
[47] *Pueblo v. Díaz, Bonano*, 176 D.P.R. 601, 612 (2009); *Pueblo v. Calderón Díaz*, 156 D.P.R. 549, 563 (2002). *Véase* Regla 11 de Procedimiento Criminal.
[48] *Pueblo v. Vázquez Méndez*, 117 D.P.R. 170, 179 (1986).

Puerto Rico busca interponer la figura del juez entre los funcionarios públicos y la ciudadanía para que las intervenciones gocen de razonabilidad, toda vez que, para el juzgador el interés en la orden es menor que el del gobierno que pretende obtener una convicción y mayor que la del sospechoso.[49] Por todo lo cual, la disposición constitucional pretende mantener un balance de poderes en virtud de la intervención de un magistrado para así garantizar la razonabilidad en la intervención del Estado en su esfuerzo de lograr una convicción y la del individuo de mantener su derecho a la intimidad.

La Constitución de Puerto Rico es custodia y guardián del derecho a la intimidad y ofrece mayores protecciones que la Constitución Federal.[50] En este contexto, la Constitución establece que "[l]a dignidad del ser humano es inviolable".[51] También, dispone que los individuos ostentan el derecho a la protección contra ataques a su honra, reputación y la vida privada y familiar.[52] El derecho a la intimidad en la Isla, opera *ex propio vigore* y puede hacerse valer tanto ante personas privadas como ante el Estado.[53] Siendo la dignidad del ser humano consustancial al derecho constitucional a la intimidad, debe "extenderse a aquellas nociones expresivas más amplias relativas al control sobre la proyección de la identidad".[54]Lo anterior significa, que el espectro del derecho a la intimidad de un individuo podría incluir "el control sobre la información personal aun cuando la misma haya sido revelada".[55]

El Tribunal Supremo de Puerto Rico, ha reiterado los tres (3) objetivos básicos del artículo II, aección 10 de la Constitución, a saber: (1) protección a la intimidad y la dignidad de los seres humanos frente a intervenciones indebidas e irrazonables por parte del Estado; (2) proteger y amparar los documentos y otras pertenencias de las personas; y (3) interponer la figura de un juez entre los funcionarios públicos y la ciudadanía, para mantener una mayoría garantía de razonabilidad a la intrusión.[56] Queda plasmada la importancia de esta garantía en la siguiente cita del Tribunal, a saber:

> Debemos decir que el temor al crimen y el natural deseo de combatirlo no deben oscurecer el propósito central de la disposición. Libremos el lenguaje original de su glosa abultada. La garantía contra los registros y allanamientos

---

[49] Chiesa Aponte, *supra* n. 6, pág. 349.

[50] *H.M.C.A. v. Contralor*, 133 D.P.R. 945, 974-75 (1993); *Pueblo v. Malavé González*, 120 D.P.R. 470, 475 (1988); *Pueblo v. Rivera Colón*, 128 D.P.R. 672, 680 (1991); *Rullán v. Fas Alzamora*, 166 D.P.R. 742, 771 (2006); *Pueblo v. Díaz Medina, Bonano*, 176 D.P.R. 601 (2009).

[51] Const. P.R. art. II, § 1.

[52] Const. P.R. art. II, § 8.

[53] *Colón* v. *Romero Barceló*, 112 D.P.R. 573 (1982); *Arroyo* v. *Rattan Specialiies,* 117 D.P.R. 35, 64 (1986).

[54] Hiram A. Meléndez Juarbe, *La Constitución en Ceros y Unos: Un acercamiento Digital al Derecho a la Intimidad y la Seguridad Pública*, 77 Rev. Jur. U.P.R. 45, 75 (2008).

[55] *Id.* pág. 79.

[56] *Pueblo v. Martínez Torres*, 120 D.P.R. 496, 500 (1988). *Véase además* Julio E. Fontanet Maldonado, *El Proceso Penal de Puerto Rico* vol. I, 92 (Editorial Inter Juris 2008).

> irrazonables representa la voluntad de negarles a los gobiernos mejor intencionados, en aras de una libertad individual preciada, medios eficaces y aun aparentemente indispensables para lograr objetivos meritorios. Se estructuró precisamente ese derecho para proteger al ciudadano aun de los gobiernos democráticos más escrupulosos.[57] Por bueno que sea el guardián, siempre existe el problema de quién lo vigila. *Quis custodiet custodiem*. Cuando se descuidan los medios, cuando se disminuyen los derechos fundamentales a nombre de un ansiado orden, lo que viene a perecer al cabo es la libertad y con ella la democracia que se quiso defender.[58]

En Puerto Rico, la protección constitucional contra registros y allanamientos irrazonables, goza de un alto estirpe y se considera que "la lesión de la intimidad es en este sentido el más penoso ataque a los derechos fundamentales de la persona".[59] Por tanto, *inter alia,* la Constitución expresamente prohíbe la intercepción de llamadas telefónicas por lo que, en comparación con la doctrina federal sobre asunción de riesgo, el derecho a la intimidad impone limitaciones de mayor alcance, en lo que respecta al uso de instrumentos tecnológicos en comunicaciones privadas. Adviértase, que esta prohibición no es absoluta, toda vez que, existen ciertas circunstancias excepcionales que ameritan la intercepción para proteger la seguridad de los individuos.[60] En ese sentido, la intervención del Estado derrotaría la prohibición de interceptar llamadas telefononicas ante aquellas circunstancias que usurpen la seguridad de la población. A su vez, no se ha extendido la prohibición sobre la intercepción de comunicaciones telefónicas y vigilancia electrónica en el lugar de trabajo, si la parte interesada en hacer la vigilancia sostiene que tiene un interés apremiante.[61] Es decir, nuestro estado de derecho requiere que la parte interesada en intersectar información privada o comunicaciones telefónicas demuestre que tiene un interés apremiante. Lo anterior significa, que en materia de registros y allanamiento, el Estado podría argüir su interés de mantener la seguridad de la población y lograr la convicción de aquellos que delinquen mediante la obtención de información cobijada por expectativa de intimidad. Ciertamente, la jurisprudencia en Puerto Rico asume una postura poética, en términos de las salvaguardas constitucionales del derecho a la intimidad. Sin embargo, al interpretar la casuística relacionada al derecho constitucional sobre la intimidad *vis a vis* el interés apremiante del Estado, la tendencia es que prevalezca el interés del Estado de proteger a la población de un atentado a la seguridad o algún interés sustancial.[62]

---

[57] Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 353 (1974).
[58] *Pueblo* v. *Lebrón*, 18 D.P.R. 324, 327-328 (1979); *Pueblo* v. *Martínez Torres*, 120 D.P.R. 496. Véase, también, *McNabb* v. *United States*, 318 U.S. 332, 347 (1943).
[59] *Diario de Sesiones de la Convención Constituyente*, vol. IV, 2323, 2567 (1952).
[60] *P.R.T.C. v. Martínez*, 114 D.P.R. 328, 359 (1983).
[61] Véase, *Vega Rodríguez v. P.R.T.C.,*156 D.P.R. 585 (2002).
[62] Camille Álvarez Jacobo, *Desvanece la Intimidad en el Mundo Virtual: La Búsqueda de Protección constitucional en Internet*, 45 Rev. Jurídica U. Inter. P.R. 265 (2010-2011).

Sin embargo, recientemente nuestro más Alto Foro, en el caso *Carlos Weber Carrillo v. Estado Libre Asociado de Puerto Rico*[63] se expresó en materia de registros sobre el derecho a la intimidad atemperado a las acciones legales de carácter civil. Así, aparte de las consideraciones procesales que versan tanto en la opinión mayoritaria por voz de la Jueza Fiol Matta y en la opinión disidente del Juez Asociado Martínez Torres,[64] el derecho sustantivo profiere un revés en cuanto a las tendencias del derecho anglosajón en lo correspondiente al derecho a la intimidad. En el caso de *Carlos Webber*, se instó una demanda contra el Estado por alegadas actuaciones en contravención al derecho a la intimidad y por daños y perjuicios. En la misma adujo que sin previa notificación ni en virtud de orden judicial, el Negociado de Investigaciones Especiales (en adelante, NIE), le solicitó a Cingular el estado mensual de las llamadas de su celular. En vista de ello, el Tribunal de Primera Instancia adopta las disposiciones del derecho común en cuanto a los registros de llamadas telefónicas y el derecho a la intimidad. Ello es así pues, determina que no se le violó al señor Webber su derecho a la intimidad respecto a su celular, toda vez que quien recibía las facturas correspondientes al servicio telefónico era su patrono y que a pesar de que tenía conocimiento del *subpoena* continuó utilizando el mismo número de teléfono y celular. A su vez, el Tribunal de Primera Instancia adopta los planteamientos antes esbozados sobre la diferencia entre la información en forma de contenido o *metadata*, por lo que concluye que no hubo intromisión indebida por parte del NIE ya que no se indagó sobre el contenido de las llamadas. Por su parte, el Tribunal de Apelaciones determinó que la obtención de información personal del señor Webber "no constituyó un registro, que el criterio de razonabilidad era suficiente para validar el requerimiento de información y que la agencia no tenía que cumplir con los controles de notificación previa u orden judicial".[65] Según podemos colegir, se proyectan consecuencias desiguales en cuanto a los planteamientos de las partes, por un lado vemos el interés del Estado en realizar el registro, obtener información y una convicción, la cual es oponible al interés de los individuos de velar por su privacidad.

En vista de lo antes expuesto, el Tribunal Supremo establece que "el derecho a la intimidad [en Puerto Rico] goza de la más alta jerarquía en nuestro ordenamiento constitucional y aplica *ex propio vigore*".[66] Además, alejándose de la interpretación de la doctrina de asunción de riesgos, añade que:

> [u]na agencia puede emitir una orden de *subpoena* para obtener documentos en manos de terceras personas para adelantar una investigación administrativa o criminal, siempre que con ello no infrinja los derechos de los investigados. De igual forma, puede requerir información perteneciente a terceros en quienes no se ha centrado la investigación, pero cuando dicho requerimiento se le

---

[63] 190 D.P.R. 688 (2014).

[64] La opinión disidente fue emitida por el Juez Asociado señor Martínez Torres a la cual se unieron la Jueza Asociada Pabón Charneco y el Juez Asociado señor Kolthoff Caraballo.

[65] *Weber Carrillo*, 190 D.P.R. págs. 695-696.

[66] *Id.* págs. 697-698.

> hace a un tercero, resulta imperante la protección judicial ante la intervención gubernamental.[67]

Por tal motivo, nuestro más Alto Foro adopta la norma de *Katz,* en cuanto a la expectativa razonable de intimidad atemperándolo al razonamiento de que "en Puerto Rico, el derecho a la intimidad tiene un alcance más amplio que en el sistema federal de Estados Unidos".[68] Por tanto, podemos colegir que el T.S.P.R., se aparta de la interpretación de que Puerto Rico goza de una factura más ancha en lo correspondiente a los derechos constitucionales, sin embargo, adopta restricciones respecto al acceso a información que es considerada como privada. Así, dispone el T.S.P.R. que el criterio rector adoptado en las controversias sobre la expectativa de intimidad incluye el análisis subjetivo acerca de si la persona afectada alberga una expectativa de intimidad sobre el lugar o el artículo a ser registrado y un análisis objetivo sobre si tal expectativa es una razonable a la luz de los criterios prevalecientes en la sociedad.[69]

En vista de lo anterior, es imperativo adaptar este análisis a los registros y allanamientos por parte del Estado para obtener una convicción, toda vez que el creciente uso de aparatos tecnológicos ha levantado un sinnúmero de interrogantes en cuanto al intercambio y publicación de información que ofrecemos a terceros. Ello es así, pues existe una bifurcación de interpretaciones judiciales entre casos criminales y civiles relacionadas a si la información que ofrecemos a terceros, aquella que guardamos en los proveedores de servicio de almacenaje en la red, cuentas de correo electrónico y redes sociales puede ser obtenida por parte del Estado como evidencia admisible en un pleito judicial. Por ejemplo, en el caso de Carlos Webber, el T.S.P.R. arguyó que al igual que en otras jurisdicciones de Estados Unidos, adoptan el planteamiento de que "al igual que las transacciones bancarias, las lista de números contenidas en una factura de teléfonos permite al Estado descubrir, con relativa facilidad, información privada de las personas,[70] incluyendo por inferencia, el contenido de la conversación".[71] Por cuanto, si adoptamos el análisis sobre la diferencia entre contenido y *metadata,* podemos razonar que debido a que en ambas instancias se puede obtener información personal, queda amparada bajo el principio de expectativa razonable de intimidad. Sin embargo, queda como interrogante si este análisis pudo haber sido adoptado si la controversia ante el Tribunal hubiese sido una de índole criminal. Así pues, estando presente en ambas controversias un derecho de estirpe constitucional, como lo es el derecho a la intimidad, habría que tomar las controversias particulares de cada caso para evaluar el grado de intromisión por parte del Estado en información personal de algún individuo. Al examinar el desarrollo

---

[67] *Id*. pág. 698.

[68] *Id.* pág. 701. *Véase además Acarón et al. v. D.R.N.A.*, 186 D.P.R. 564, 573 (2012).

[69] *Id*.

[70] *Id. Véase además Commonwealth v. Melilli,* 555 A.2d 1254 (Pa. 1989); *People v. Spoleder*, 666 P.2d. 135 (Colo. 1983); *State v. Hunt*, 450 A.2d 952 (N.J. 1982).

[71] *Weber Carrillo*, 190 D.P.R. pág. 712.

jurisprudencial en lo referente a casos criminales en Puerto Rico, ciertamente podemos apreciar una discrepancia sobre la amplitud de la expectativa de intimidad a la que hace referencia el caso de *Carlos Webber*, toda vez que la jurisprudencia más reciente sobre casos criminales ha conferido mayores herramientas para el Estado obtener una convicción bajo el interes apremiante de salvaguardar la seguridad de la población.[72] Por tal motivo, forzoso es concluir que los avances tecnológicos se han convertido en una herramienta de información masiva, en los que el Estado puede adquirir información personal y la misma puede ser utilizada como evidencia admisible sin previa orden judicial.

Finalmente, los teléfonos móviles se han convertido en G.P.S., los correos electrónicos y los servicios en la red en base de datos, así como las redes sociales se han convertido en fichas sobre personalidad, gustos, opiniones, creencias religiosas, convicciones políticas, *inter alia,* de las personas que acceden a los términos y condiciones de los proveedores de estos servicios. Consecuentemente, estos servicios se han convertido en herramientas investigativas para el Estado, debido a la extraordinaria utilidad para acceder a información considerada privada, personal e íntima

III. Conclusión

Las innovaciones de la era digital, han traído consigo el desarrollo exponencial de tecnología al alcance de la mayoría de la población, en especial, de los países desarrollados. Estos adelantos tecnológicos, se han convertido en herramientas necesarias para completar tareas u obligaciones cotidianas. Así, la tecnología se ha convertido en una especie de mano derecha en la que confiamos nuestra información privilegiada o confidencial, realizamos transacciones bancarias, compartimos comunicaciones privadas, organizamos nuestros calendarios, accedemos nuestras cuentas en las redes sociales, entre otras. Por cuanto, si partimos de la premisa sobre el uso cotidiano de instrumentos tecnológicos como tabletas, GPS, *iClouds,* computadoras, *Smartphones*, entre otros, preciso es señalar que incrementa la expectativa de intimidad sobre la información que intercambiamos con los terceros debido al uso necesario de estos. En vista de ello, podríamos concluir que en esta era digital en la que el intercambio y la intromisión de terceros es variante, existe una serie de nivelaciones relacionadas a la expectativa de intimidad. Es decir, que podría darse la variación en dos (2) instancias, a saber: (a) tipo de información compartida en forma de contenido o *metadata*; y (b) la cantidad de receptores a los que comunico cierta información.

A modo ilustrativo, imaginemos que compartimos cierta información acerca de un evento importante en nuestras vidas, así detallamos cada preciso momento con lujo de detalles, al mismo tiempo, incluimos como receptores del mensaje a todo el grupo

---

[72] *Véase Pueblo v. Báez López*, 189 D.P.R. 918 (2013); *Pueblo v. Fernández Rodríguez*, 188 D.P.R. 165 (2013); *Pueblo v. Díaz Medina*, 176 D.P.R. 601 (2009).

de amigos incluidos en la cuenta de Facebook. Al analizar este caso bajo el crisol de la Cuarta Enmienda y la jurisprudencia norteamericana, ciertamente se trata de la difusión de información a modo de contenido. Por otro lado, al analizar el número de receptores del mensaje, es forzoso concluir que el nivel de expectativa de intimidad se encuentra considerablemente reducido, toda vez que, las oportunidades de que el receptor comparta la información con un tercero es altamente probable. Así pues, en este caso el registro de la presente comunicación, por parte del Estado, no estaría cobijado por la Cuarta Enmienda.

Por el contrario, en la forma y manera en que se utilizan los aparatos electrónicos, para hacer transacciones en línea con la entidad financiera, la parte que realiza la gestión tiene que pasar por un proceso de autenticación en la que brinda información personal y datos que ciertamente guardan una expectativa de intimidad debido a su contenido. Asimismo, la rigurosidad de poder acceder a la cuenta bancaria en la red, debe subsanar la asunción de riesgo al compartir cierta información con la entidad bancaria o el llamado tercero.

Por todo lo cual, debido al continuo desarrollo de la tecnología y la utilización de estas herramientas electrónicas para gestiones cotidianas, es evidente que la legislatura debe desarrollar estatutos que cobijen bajo su mandato la expectativa razonable de intimidad que posee la población en general, a la hora de compartir información personal con terceros. Es decir, que se elaboren restricciones prudentes de acuerdo a la información intercambiada, para que no sea libremente compartida con el Estado y se mantenga vigente una Cuarta Enmienda más inclusiva y acomodada a los avances tecnológicos. A su vez, debe limitar la discreción que ostentan los proveedores de servicios en la red para diseñar los términos y condiciones además de la liberalidad que poseen para cambiar aleatoriamente los mismos. Todo lo anterior lo realizan estas compañías sin el previo consentimiento y notificación a los usuarios de tales servicios. Por otra parte, los tribunales deben mantener su rol de celosos guardianes de la constitución y custodiar los derechos adquiridos por la población en virtud de la expectativa razonable de intimidad. Es decir, los tribunales pueden contribuir a estandarizar, por medio de la jurisprudencia, las limitaciones o atribuciones que posee el Estado para acceder a información concerniente a datos personales provistos o compartidos en la red.