LAS REDES SOCIALES Y LAS ÓRDENES DE REGISTRO Y ALLANAMIENTO: UNA MIRADA A LA EXPECTATIVA RAZONABLE DE INTIMIDAD

ARTÍCULO

ANA M. BATISTA,* JOAN M. GONZÁLEZ** Y BARBIE L. ROMÁN***

* La autora es egresada del programa nocturno de la Escuela de Derecho de la Universidad de Puerto Rico, clase 2021. Se graduó con Altos Honores. Durante sus estudios perteneció al Pro Bono Acceso Derecho UPR y a la Asociación de Litigio de la Universidad de Puerto Rico. Admitida al ejercicio de la Abogacía en Puerto Rico, el 29 de enero de 2022.
** La autora es egresada del programa nocturno de la Escuela de Derecho de la Universidad de Puerto Rico. Fue vicepresidenta nocturna de la clase 2021. Se graduó con Altos Honores y durante sus estudios perteneció al Pro Bono Acceso Derecho UPR. Admitida al ejercicio de la Abogacía en PR, el 29 de enero de 2022.
*** La autora es egresada del programa nocturno de la Escuela de Derecho de la Universidad de Puerto Rico, clase 2021. Se graduó con Honores. Durante sus estudios perteneció al Pro Bono Acceso Derecho UPR, y al Taller de Práctica Legal, asignada a la Sociedad de Asistencia Legal, etapa apelativa.

Introducción

Las últimas dos décadas han traído consigo avances significativos en las comunicaciones electrónicas a través de la Internet. Los avances más recientes han logrado que las redes sociales sean los servicios de comunicación más populares y utilizados a nivel mundial. En efecto, la mayoría de los puertorriqueños utilizan al menos una red social. Estas redes se han convertido en un mecanismo donde se desarrollan relaciones interpersonales y en un instrumento de comunicación que utilizamos a diario, donde compartimos nuestra información, fotos, videos y escritos con otros usuarios.

El objetivo de las redes sociales es conectar al mundo. Una red social es una herramienta en línea para comunicarse y transmitir información. También permite que los usuarios se envíen mensajes directos entre ellos. Sin embargo, para su funcionamiento, los proveedores de estos servicios archivan la actividad de sus usuarios, tanto el contenido que comparten como las transacciones que realizan. Sus usuarios quieren abrirse a estas nuevas tecnologías, pero también desean preservar su privacidad.[1] Es cierto que las redes sociales ofrecen a sus usuarios cierto control sobre la información que comparten a través de configuraciones de privacidad. Sin embargo, estas configuraciones de privacidad pueden no ser confiables.

En la actualidad, las personas comparten todo tipo de información a través de sus redes sociales. "En el 2018, alrededor de siete de cada diez estadounidenses usaban algún tipo de red social".[2] En el 2019, sobre 3.4 mil millones de personas en el mundo tenían algún tipo de presencia en el Internet, y se proyecta que la cantidad crezca a casi 4.12 mil millones para el 2023.[3]

Los avances en este contexto traen consigo ciertas interrogantes como ¿qué expectativa de privacidad puede tener un usuario sobre la información compartida en las redes sociales?; ¿cuándo se activa la protección constitucional contra los registros y allanamientos irrazonables?, y ¿qué leyes aplican a las comunicaciones hechas a través de estas plataformas?

En los Estados Unidos hay opiniones divididas en cuanto a la aplicabilidad del derecho a la intimidad en las redes. Algunos argumentan que carece de la protección constitucional de la Cuarta Enmienda contra los registros y allanamientos irrazonables; mientras otros creen que hay que ver caso a caso y el tipo de red social en cuestión.

Este artículo pretende contestar las interrogantes antes mencionadas en cuatro partes. En la primera parte, discutiremos la Constitución de Estados Unidos y su protección a la privacidad bajo la Cuarta Enmienda, así como las leyes aplicables a las comunicaciones electrónicas.[4] En la parte II comenzamos a adentrar en el mundo de las redes sociales,

---

1 Elissa M. Torres Soto, *Una Nueva Mirada al Derecho de la Intimidad: Las Redes Sociales*, 57 Rev. D.P. 357, 358-59 (2018).

2 Alessandra P. Serano & Joseph J. M. Orabona, *Using Social Media Evidence at Trial,* 67 DOJ J. Fed. L. & Prac. 135 (2019) (traducción suplida).

3 *Number of social network users worldwide from 2017 to 2025 (in billions),* Statista, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (última visita 15 de marzo de 2022).

4 Debido a la falta de jurisprudencia de Puerto Rico en estos temas, este artículo se concentra en el análisis de las protecciones establecidas por la Constitución de Estados Unidos, su jurisprudencia y las leyes federales sobre el tema en discusión.

en específico las redes de comunicación y promoción comercial más grandes al momento: *Facebook* e *Instagram*. La parte III examina las redes de mensajería instantánea más populares: *Messenger*, *WhatsApp* y *Telegram*. La parte IV le da el turno a las redes de mensajería efímera como lo son *Snapchat* y *TikTok*. En cada parte, veremos las políticas de privacidad de cada red social discutida y cómo los tribunales han aplicado la doctrina de la expectativa razonable de intimidad a estas, bajo la protección de la Cuarta Enmienda. Finalmente, en la parte V, se discutirán propuestas jurídicas que buscan remediar la discordancia entre las leyes disponibles —en efecto atrasadas— para tratar estos tipos de tecnología, junto con el balance que se debe obtener y mantener para salvaguardar la privacidad y el derecho a la intimidad de las personas dentro del mundo cibernético de las redes sociales.

I. Protección constitucional y de ley a la expectativa razonable de intimidad

A. La Constitución y la jurisprudencia

El artículo II, sección 10 de la Constitución del Estado Libre Asociado de Puerto Rico establece la protección que tienen las personas en contra de registros, incautaciones y allanamientos irrazonables.[5] Además, expone que: "[s]ólo 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".[6] Esta garantía constitucional va de la mano con el derecho a la intimidad, el cual se encuentra en el artículo II, sección 8 de nuestra Constitución.[7]

En la Constitución de los Estados Unidos este derecho se encuentra establecido bajo la Cuarta Enmienda.[8] Esta enmienda "protege dos derechos fundamentales: el derecho a la privacidad y el derecho a no sufrir una invasión arbitraria".[9] La misma expone que:

> El derecho del pueblo a la seguridad que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán órdenes, excepto con motivo probable, sustentados mediante juramento o promesa, y expresamente describiendo el lugar que será registrado y las personas o cosas que han de ser detenidas o incautadas.[10]

---

5 Const. PR art. II, § 10.

6 *Id.*

7 Const. PR art. II, § 8; Emmanuel Caballer Roig, *Registros y allanamientos: El tráfico de información en Internet*, 56 Rev. D.P. 261, 264-65 (2017).

8 Const. EE. UU. enm. IV.

9 *Legislación sobre pesquisas y confiscaciones cuarta enmienda,* Legal Inf. Inst., https://www.law.cornell.edu/wex/es/legislación_sobre_pesquisas_y_confiscaciones_cuarta_enmienda (última visita 15 de marzo de 2022).

10 Const. EE. UU. enm. IV (traducción obtenida de: *The Constitution of the United States: En Espanol*, Nat'l Const. Ctr, https://constitutioncenter.org/learn/educational-resources/historical-documents/the-constitution-of-the-united-states-html-en-espanol (última visita 15 de marzo de 2022)).

La Cuarta Enmienda hace la contribución distintiva de proteger la privacidad del individuo y regular las instituciones —como la policía— que con más probabilidad invadirían esa privacidad.[11] Esta enmienda, y el derecho a la intimidad que la misma protege, ha sido sujeta a interpretación extensa por el Tribunal Supremo de los Estados Unidos. El caso normativo para la aplicación de la misma es el caso de *Katz,* donde el más alto foro federal estableció que la piedra angular del derecho a la intimidad es la razonabilidad.[12]

En este caso, el Tribunal Supremo de Estados Unidos trazó una nueva línea, estableciendo los actuales principios básicos en la jurisprudencia de la Cuarta Enmienda: que la Cuarta Enmienda protege personas y no propiedades,[13] y que aplica solo en instancias donde el individuo tiene una expectativa razonable de intimidad.[14] El requisito de necesitar una orden judicial de registro y allanamiento bajo la Cuarta Enmienda es activado cuando un registro traspasaría la expectativa razonable de intimidad del individuo.[15] La opinión concurrente del juez Harlan en *Katz* expresó que habría que determinar si existe una expectativa de intimidad tanto subjetiva como objetiva.[16] Esto implica que la persona demuestre su intención de tener esa expectativa de privacidad —subjetiva— y que la sociedad reconozca que ese reclamo a la privacidad es razonable —objetiva—.[17] Esto fue acogido por nuestro Tribunal Supremo en el caso de *Pueblo v. Ortiz Rodríguez*.[18]

Es importante señalar que deben concurrir ambos criterios para que se establezca que hay una expectativa de intimidad razonable. El foco principal del examen de estos criterios recae sobre la expectativa razonable de privacidad *objetiva*. "La legitimidad de la expectativa de privacidad debe tener una fuente ajena a la Cuarta Enmienda, ya sea por conceptos de derechos reales o personales o a preceptos que han sido reconocidos y permitidos por la sociedad".[19] En *Smith v . Maryland*, el Tribunal Supremo expresó que todo lo que una persona voluntariamente exponga al público no puede estar sujeto a la protección de la Cuarta Enmienda,[20] lo que parece indicar que una vez divulgada la información, no importa el contexto, ya no puede ser considerada como privada. Esta decisión, al ser aplicada a la tecnología actual, da a entender que la protección de la Cuarta Enmienda no aplica a lo que hoy conocemos como *metadata* —información que se recopila y usa para operar u obtener ciertos productos o servicios—.[21]

Los nuevos adelantos tecnológicos presuponen un reto para el tema del derecho a la intimidad. El Derecho debe adaptarse a las nuevas circunstancias tecnológicas. En su opinión concurrente en el caso de *U.S. v. Jones*, la honorable jueza Sotomayor expuso que es necesario que se revise la premisa que la información voluntariamente vertida a terceras

---

11 Thomas P. Crocker, *The Political Fourth Amendment*, 88 Wash. U. L. Rev. 303, 310 (2010).
12 Katz v. United States, 389 U.S. 347 (1967).
13 *Id.* en la pág. 351.
14 *Id.* en la pág. 353.
15 Rakas v. Illinois, 439 U.S. 128, 151 (1978).
16 *Katz*, 389 U.S. en la pág. 361 (Harlan, opinión concurrente).
17 Torres Soto, *supra* nota 1, en las págs. 363-64.
18 Pueblo v. Ortiz Rodríguez, 147 DPR 433 (1999).
19 *Rakas,* 439 U.S. en las págs. 143-44 (traducción suplida).
20 Smith v. Maryland, 442 U.S. 735, 743-44 (1979); *véase* Kelsey Joy Smith, *The Constitutional Right to Deletion: The Latest Battle in the War of Technology v. Privacy*, 42 New Eng. J. on Crim. & Civ. Confinement 121, 123-24 (2016).
21 *Smith*, 442 U.S. en las págs. 743-44 (a esto se le conoce como el *third-party doctrine*).

personas está desprovista del derecho a la intimidad.[22] La Jueza expone que esto es inconsistente con los avances tecnológicos actuales en los que las personas a través de los medios digitales revelan mucha información a terceras personas.[23]

B. Las leyes aplicables y las ordenes de registro

La nueva realidad tecnológica ha causado un aumento significativo en el almacenamiento de información electrónica. Esta evidencia digital ha provocado un reto para el derecho a la intimidad. Si bien las comunicaciones electrónicas son fuentes valiosas de información, los registros a dicha información, aún con orden judicial, pueden socavar los derechos contenidos en la Cuarta Enmienda. En los registros de evidencia digital normalmente se obtiene mucha información electrónica que abarca más de lo que es pertinente y está al alcance de la orden judicial. Hay que siempre poner en una balanza los intereses de privacidad del usuario versus la capacidad del gobierno de llevar a cabo una búsqueda efectiva.[24]

El Congreso, hace más de veinte años, aprobó una serie de legislaciones necesarias para enfrentar el avance de la digitalización de la época y el problema enfrentado con las nuevas comunicaciones electrónicas.

i. Electronic Communications and Privacy Act

La *Electronic Communications and Privacy Act* (en adelante, "E.C.P.A.") fue aprobada en el 1986, como respuesta a los avances tecnológicos de la época. La ley contiene tres secciones: (1) *Wiretap Act*;[25] (2) *Stored Communications Act*,[26] y (3) *Pen Register Act*.[27] Antes de que se aprobara esta ley, el Tribunal Supremo había expresado en una serie de casos que la divulgación de información personal a los negocios quedaba fuera de la protección a la privacidad de la Cuarta Enmienda.[28] Esto resultó problemático más tarde, al expandirse el uso de los correos electrónicos y otros servicios, en los que era necesario que el usuario divulgara su información personal a los proveedores para obtener sus servicios. Es dentro de este marco de riesgo a la privacidad de los ciudadanos que se aprueba la Ley.

Las cuentas de las redes sociales son un tipo de información electrónica almacenada. El acceso del gobierno a la información almacenada electrónicamente se rige por la *Stored Communications Act* (en adelante, "S.C.A."), ley que es parte de la E.C.P.A.[29] La S.C.A.

---

22 United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, opinión concurrente); *véase* Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 Miss. C. L. Rev. 227, 240-41 (2012).

23 *Jones*, 565 U.S. en la pág. 417.

24 Sara J. Dennis, *Regulating Search Warrant Execution Procedure for Stored Electronic Communications*, 86 Fordham L. Rev. 2993 (2018).

25 Electronic Communications and Privacy Act, 18 U.S.C. §§ 2510-2523 (2012).

26 *Id.* §§ 2701-2712.

27 *Id.* §§ 3121-3127.

28 Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1562 (2004).

29 Electronic Communications and Privacy Act, 18 U.S.C. §§ 2701-2712 (2012); *véase* Emmanuel Caballer Roig, *Registros y allanamientos: El tráfico de información en Internet*, 56 Rev. D.P. 261, 270-72 (2017).

fue aprobada en parte para limitar el poder del gobierno de requerir la divulgación de información por parte de terceros proveedores de servicios de internet,[30] aunque también identifica cuándo las agencias gubernamentales de ley y orden pueden tener acceso a dicha información.[31] La sección 2703 de esta ley faculta a las agencias de ley y orden a exigirle a un proveedor de servicios de información electrónica que revele el contenido de cualquier comunicación electrónica. Estos pueden obtener una amplia gama de información sin solicitar una orden judicial; sin embargo, el tener una orden de registro y allanamiento les facilita obtener el tipo y la cantidad de información que desean. De acuerdo con esta ley, un oficial debe determinar dos cosas antes de requerir que un proveedor emita la información. Estas dos determinaciones son importantes ya que de estas depende la facilidad con la que el gobierno puede acceder a la información electrónica.

Lo primero es determinar el tipo de proveedor. La S.C.A. cubre una gama de proveedores de servicios electrónicos, tales como proveedores de correo electrónico, empresas de redes sociales, y servicios de aplicaciones de mensajería. La Ley agrupa a los proveedores de información en dos grupos, según los servicios que ofrecen: los que proveen servicios de comunicación electrónica (en adelante, "ECS", por sus siglas en inglés), donde los usuarios tienen la capacidad de enviar o recibir comunicaciones electrónicas, y los que proveen servicios de computación remota, (en adelante, "RCS", por sus siglas en inglés), los cuales brindan al público servicios de almacenamiento o procesamiento de computadoras por medio de un sistema de comunicaciones electrónicas. La distinción entre ambos es importante, pues la facilidad de acceso a la información depende de esa clasificación. Los oficiales pueden obtener información de un proveedor categorizado como RCS si obtienen una orden de registro bajo la Regla 41 o utilizan el procedimiento de citación establecido en la sección 2703 (b) (1) (B) de la ley.[32] En cambio, la información en poder de un proveedor ECS que tenga 180 días o menos de existencia solo se puede acceder con una orden judicial obtenida de conformidad con la Regla 41.[33] Si tiene 181 días o más, la comunicación se trata como contenido almacenado con un RCS. Es muy complicado definir el tipo de un servidor.[34] De hecho, hoy día hay redes sociales que se pueden interpretar como un ECS y un RCS a la vez, lo que les ofrece una amplia discreción a los oficiales. En fin, la disponibilidad de información depende del proveedor y del tipo de cuenta electrónica.

Segundo, debe determinar el tipo de información buscada para, de esta manera, establecer qué herramientas se deben usar para requerir al proveedor que emita la información. La ley clasifica la información en tres categorías: (1) información básica del usuario, (2) registros del usuario, y (3) información del contenido de la comunicación; esta clasificación determina el grado de acceso que tendrá el oficial.[35] Bajo la primera categoría, información sobre la identidad del usuario, el proveedor debe dar la información después de recibir una citación o *subpoena*.[36] Para la segunda categoría, registros de las transacciones

---

30 Ryan A. Ward, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 Harv. J.L. & Tech. 563, 566 (2011).
31 Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1413 (2004).
32 18 U.S.C. § 2703(b) (2012).
33 *Id.* § 2703(a).
34 *Id.*
35 *Id.* §2703(c).
36 *Id.*

que hizo el usuario, listas de sitios web que accedió, etc., el proveedor debe dar la información si el oficial tiene una orden de registro conforme a la Regla 41 de Procedimiento Criminal Federal o una orden especial bajo la sección 2703 (d) de esta ley.[37] En la tercera categoría, la información de contenido, el proveedor dará la misma, solo si hay una orden judicial de registro.[38]

Aunque la ley no siempre requiere una orden de registro para que el oficial pueda obligar la divulgación, es lo conveniente para evitar posibles conflictos. Generalmente, una orden especifica la cuenta desde la cual se buscan las comunicaciones y también puede incluir un rango de fechas pertinentes o tipos específicos de datos. No se requiere que el oficial esté presente en la recopilación de la información, sino que el proveedor le puede hacer llegar a este una copia de lo solicitado.[39] Caballer Roig establece que:

> Las disposiciones de la S.C.A. deberían aplicar a Puerto Rico, . . . su efecto sería en cuanto al diligenciamiento de la orden de registro, . . . limitado a la información de contenido digital. Puerto Rico podría adoptar una ley que sea más rigurosa en cuanto al requisito de causa probable y el diligenciamiento de la orden, pero no menos de las disposiciones del S.C.A.[40]

Una solicitud para una orden de registro y allanamiento debe contener causa probable, descripción de lo que se busca y declaración jurada, sea esta para contenido electrónico o no.[41] Sin embargo, una orden judicial de información electrónica tiene múltiples características que la distinguen de una orden judicial estándar. La enmienda de 2009 a la Regla 41 de Procedimiento Criminal Federal permite un proceso diferente para obtener información electrónica almacenada.[42] Esta enmienda crea un proceso de dos pasos que deben seguir los oficiales que van a ejecutar el registro. Primero, la policía debe adquirir la información electrónica almacenada (en adelante, "ESI" por sus siglas en inglés) del lugar donde se almacena y luego realizar una revisión de esta información para depurarla y determinar qué de esta es relevante a su caso.[43] La Regla 41 limita el período de tiempo para ejecutar la orden a catorce días,[44] pero no impone limitaciones a la cantidad de tiempo que los investigadores pueden retener los datos para fines de revisión.

ii. Communications Assistance For Law Enforcement Act

En el 1994, el Congreso de los Estados Unidos aprobó la *Communications Assistance For Law Enforcement Act* (en adelante, "C.A.L.E.A.").[45] Esta ley requería que los provee-

---

37 *Id.*
38 *Id.*; *véase* Dennis, *supra* nota 24, en las págs. 2997-3001.
39 *Id*.
40 Emmanuel Caballer Roig, *Registros y allanamientos: El tráfico de información en Internet*, 56 Rev. D.P. 261, 276 (2017).
41 Fed. R. Crim. P. 41.
42 *Id.* R. 41(e)(B).
43 Reid Day, *Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services*, 64 U. Kan. L. Rev. 491, 509 (2015).
44 Fed. R. Crim. P. 41(e)(2)(i).
45 Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010 (2012).

dores de telecomunicaciones se aseguraran de que el gobierno pudiera intervenir conversaciones telefónicas, comúnmente conocido por su palabra en inglés, *wiretaps*. La ley fue escrita para enfrentar un problema en específico: mientras las telecomunicaciones cambiaban del sistema análogo al sistema digital, se dificultaba más el que las mismas compañías pudieran cumplir con las órdenes judiciales de intervención.[46] Para resolver el problema, C.A.L.E.A. requeriría que los proveedores de telecomunicaciones usaran equipo que tuviera la capacidad de apoyar intervenciones legales.[47] A pesar de que la ley tuvo un propósito estrecho y demarcado, esta contiene dentro de sus requerimientos, varios preceptos notables. Uno de estos preceptos es que, dentro de sus requerimientos, se mantiene la división entre el contenido de la comunicación y la *metadata*,[48] según establecido por los casos de *New York Telephone Co.* y *Smith*.[49] Otro aspecto notable de C.A.L.E.A. es el simple hecho de su existencia. El Congreso de los Estados Unidos nunca había impuesto la responsabilidad a compañías privadas de asegurar que sus negocios o tecnologías ayudaran a las agencias de ley y orden. C.A.L.E.A. fue posiblemente la primera vez que el Congreso impuso a las compañías requisitos afirmativos de diseño de forma que apoyaran al Estado y a sus agencias de ley y orden.[50] Aunque la ley no incluía obligación alguna relacionada al Internet, en el 2004 el Departamento de Justicia Federal ("DOJ", por sus siglas en inglés), la Oficina Federal de Investigaciones ("FBI", por sus siglas en inglés), y la Administración para el Control de Drogas ("DEA", por sus siglas en inglés) pidieron a la Comisión Federal de Comunicaciones ("FCC", por sus siglas en inglés) que clasificara los servicios de *Voice over Internet Protocol* (VoIP) como servicios de telecomunicación para los efectos de la C.A.L.E.A. La FCC determinó que ciertos proveedores de servicios de VoIP —aquellos que estén interconectados con redes telefónicas tradicionales— estarían sujetos a los requisitos de la C.A.L.E.A.

Aunque algunos entienden que C.A.L.E.A. fue una enmienda al E.C.P.A., esta dejó partes de la ley como la *Wiretap Act* y la *Pen Register Act* intactos, y no ocasionó grandes cambios al *Stored Communications Act*.[51] La ley tampoco se expresa respecto a los artefactos electrónicos usados y controlados por individuos. Nada en la E.C.P.A. aplica a la información guardada en un artefacto personal. Cualquier acceso del Estado a estos equipos está regido primordialmente por las enmiendas Cuarta y Quinta de la Constitución.[52] De la misma forma, C.A.L.E.A. tampoco impone obligación alguna en los manufactureros de estos equipos y artefactos, incluso en aquellos que manufacturan equipos de telecomunicación.[53] Aun con sus limitaciones, C.A.L.E.A. ha sido reconocida como el esfuerzo legislativo más sustancial, hasta el momento, para abordar los efectos de los cambios en la tecnología de las telecomunicaciones y el acceso del Estado a ese tipo de información.[54]

---

46 Justin Hurwitz, *Encryption Congress mod (Apple + CALEA)*, 30 Harv. J. L. & Tech. 355, 373 (2017).
47 *Id.* en la pág. 373.
48 *Id.* en la pág. 378.
49 United States v. New York Tel. Co., 434 U.S. 159 (1977); Smith v. Maryland, 442 U.S. 735 (1979).
50 Hurwitz, *supra* nota 46, en la pág. 379.
51 *Id.* en la pág. 385.
52 *Id.*
53 *Id.*
54 *Id.* en la pág. 360.

"En resumen, C.A.L.E.A. y la E.C.P.A. trabajan en conjunto para determinar la información electrónica a la que tiene acceso el Estado, aunque no siempre conllevan el propósito de proteger la privacidad de los ciudadanos".[55] La tecnología de las comunicaciones continúa avanzando a pasos agigantados desde la aprobación de estos estatutos. Ambas leyes fueron aprobadas antes de la era digital actual y, al no estar actualizadas aún, representan una amenaza, tanto para los ciudadanos que reclaman su derecho a la privacidad, como para el oficial de ley que requiere de información pertinente para sus investigaciones.[56] "Este vacío en las leyes y jurisprudencia fomenta que haya diferencias en las interpretaciones sobre los derechos que los ciudadanos tienen respecto a sus comunicaciones a través del Internet",[57] y a su vez en sus comunicaciones e interacciones en las redes sociales.

Cabe señalar que, históricamente, las cortes han preferido aquellos métodos de vigilancia que van a fin con la protección de la Cuarta Enmienda sobre aquellos que son simplemente convenientes al Estado.[58] Los derechos a la privacidad e intimidad tienen precedencia ya que impactan valores fundamentales de una sociedad libre, como lo son la libertad de expresión y de asociación. El Tribunal Supremo ha dado énfasis especial al derecho a la intimidad en la jurisprudencia de la Cuarta Enmienda, expresando que la seguridad de la privacidad del individuo protegida en contra de la intrusión arbitraria por la policía —lo cual es el fundamento de la Cuarta Enmienda— es básico para una sociedad libre.[59]

Teniendo esto en mente, pasamos a discutir algunas de las redes sociales más populares,[60] y cómo estas han sido vistas a través del lente de las leyes y de la Constitución.

II. Redes Sociales de Comunicación y Promoción Comercial

A. Facebook

Facebook es la red social líder en el mercado, la cual cuenta con aproximadamente 1.79 billones de usuarios activos.[61] "Esta permite a sus usuarios crear perfiles individuales con ciertas configuraciones de privacidad para autoseleccionar una audiencia para el contenido que comparte en su página".[62] Es decir que, en *Facebook*, para poder tener acceso a la información de otra persona se necesita ser su "amigo". Claro está, que si el usuario escoge que su perfil sea público, entonces cualquier persona podría ver la página sin necesidad de ser su "amigo".[63] Estos son los perfiles que se consideran que no están limitados por

---

55 Shannon Gross, *A Mystery Wrapped in an Encryption: Surveillance and Privacy in the Encrypted Era*, 15 Nw. J. Tech. & Intell. Prop. 73, 82 (2017) (traducción suplida).
56 *Id.*
57 *Id.*
58 *Véase* Berger v. New York, 388 U.S. 41, 53 (1967).
59 Wolf v. Colorado, 338 U.S. 25, 28 (1949).
60 *Véase* Simon Kemp, *Digital 2020: 3.8 Billion People Use Social Media*, We Are Social (30 de enero de 2020), https://wearesocial.com/uk/blog/2020/01/digital-2020-3-8-billion-people-use-social-media/.
61 Torres Soto, *supra* nota 1, en la pág. 365.
62 Agnieszka A. McPeak, *The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data*, 48 Wake Forest L. Rev. 887, 894 (2013) (traducción suplida).
63 Torres Soto, *supra* nota 1, en la pág. 366.

ningún tipo de restricción de privacidad. En cambio, hay usuarios que permiten que solo sus amigos vean su contenido.

Facebook es una red social multifacética ya que le permite a sus usuarios, además de comunicarse y recibir mensajes personales, acceder a terceras aplicaciones a través de esta; en fin, sus usuarios pueden realizar diversas tareas.[64] Las redes sociales, incluyendo *Facebook*, proveen configuraciones de privacidad que pretenden dar a sus usuarios algún control sobre quién ve su información personal.[65] La mayoría de los usuarios de *Facebook,* conocen y utilizan al menos algunos de los mecanismos de privacidad disponibles.[66] *Facebook* constantemente renueva estas configuraciones de privacidad y aclara en los términos de uso que no es responsable de garantizar la privacidad del usuario.[67] Estas configuraciones distinguen las publicaciones públicas de las privadas.[68] Los límites de privacidad que un usuario afirmativamente escoge en su cuenta para limitar las personas que ven su contenido no siempre funcionan.[69] Esto debido a que, si un amigo comenta sobre la publicación del usuario, los amigos de ese amigo pueden ver la publicación original.[70] De esta manera, terceros ven su publicación sin ser sus amigos.[71] De la misma manera si un usuario etiqueta a un amigo en una foto o publicación, esa foto también puede aparecer en la página de ese amigo y de esta manera ser visto por terceros.[72]

Igualmente, el que la persona haya puesto su perfil como privado no impide que los oficiales de la ley y el orden obtengan la información de su cuenta.[73] Lo cierto es que se ve caso a caso. La tendencia es que la información de la cuenta de un usuario se considera pública a menos que el usuario afirmativamente opte por activar alguna restricción de privacidad.

En el caso de *United States v. Meregildo,* el tribunal expresó que un usuario que utiliza configuraciones de privacidad en su cuenta tiene expectativa razonable de privacidad, ya que el activarlo refleja su intención de preservar su contenido como privado y por lo tanto está protegido bajo la Cuarta Enmienda.[74] En este caso, el usuario mantuvo un perfil de *Facebook* en el que le permitió a sus amigos en la red ver una lista de todos sus otros amigos de *Facebook*, así como sus publicaciones.[75] El Estado logró ver el perfil del acusado en *Facebook* a través de la cuenta de uno de sus amigos, y así tuvo acceso a la evidencia que justificó la orden de registro.[76] Si el usuario permite que sus amigos en la aplicación vean su información, el Gobierno puede acceder a ellas a través del perfil de ese amigo sin violar

---

64 McPeak, *supra* nota 62, en la pág. 894.
65 *Id.* en la pág. 892.
66 *Id.* en la pág. 897.
67 *Id.* en las págs. 897-98.
68 *Id.* en la pág. 898.
69 *Id.* en la pág. 900.
70 *Id.*
71 *Id.*
72 *Id.*
73 *Id.* en la pág. 899.
74 United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012).
75 *Id.*
76 *Id.* en las págs. 525-26.

la Cuarta Enmienda.[77] En otras palabras, el limitar el perfil de *Facebook* no le asegura completamente al usuario, que sus amigos lo mantengan privado. Cuanto más amplio sea el círculo de amigos, mayor probabilidad hay de que las publicaciones sean vistas por alguien quien el usuario nunca esperaba que lo viera.[78] La expectativa de privacidad del usuario, según este caso, termina cuando difunde sus publicaciones a sus amigos porque esos amigos son libres de usar la información como quisieran.[79]

En el caso de *Reid v. Ingerman Smith LLP* el tribunal del Distrito Federal de Nueva York citó a *Meregildo* y estuvo de acuerdo con que la expectativa de privacidad no puede asegurarse cuando se comparte las publicaciones con los amigos.[80] En este caso, los demandados exigían que el tribunal ordenara la divulgación del contenido de las publicaciones hechas por el demandante en su página de *Facebook* ya que argumentaban que estas publicaciones contradecían las afirmaciones del demandante de que sufría angustias mentales por un presunto acoso sexual y terminación de empleo.[81] El tribunal se negó a exigir la divulgación de todo el contenido de la red social del demandante y lo limitó a aquellas relevantes al reclamo.[82]

Por otro lado, ha surgido la controversia de que el mismo *Facebook* se ha negado a proveer la información de sus usuarios. En el caso de *381 Search Warrants Directed to Facebook, Inc.*, la Corte Suprema de Nueva York emitió 381 órdenes de registro dirigidas a *Facebook*. [83] Estas buscaban la información de subscriptores y el contenido de numerosas cuentas de usuarios relacionados a una investigación penal. *Facebook* se negó.[84] Argumentó que las órdenes eran constitucionalmente defectuosas por ser excesivas y carentes de particularidad.[85] El tribunal desestimó el reclamo de *Facebook*, por lo que este tuvo que cumplir con la orden y suministrar la data.[86] Por el contrario, en el caso *In the Matter of Search of Information Associated with Facebook Account Identified by the username Aaron. Alexis*, la corte dictaminó que el Gobierno tenía que minimizar la cantidad de información que sus órdenes de registro trataban de obtener.[87] Para cumplir con esto, expresó que las órdenes de registro deben adaptar parámetros que eviten ser generales ya que estos violan la Cuarta Enmienda.[88]

---

77 *Id.* en la pág. 526.
78 *Id.*
79 *Id.*
80 Reid v. Ingerman Smith LLP, No. CV 0307, 2012 WL 6720752, en la pág. *2 (E.D.N.Y. 27 de diciembre de 2012); Remington M. Angelle, *Navigating the Marshes Through the Thick Fog of Reasonable Expectations of Privacy & Jurisprudence: Social Media Records Discovery in Louisiana*, 44 S.U. L. Rev. 292, 312 (2017).
81 *Reid*, No. CV 2012-0307, en la pág *1.
82 Remington M. Angelle, *Navigating the Marshes Through the Thick Fog of Reasonable Expectations of Privacy & Jurisprudence: Social Media Records Discovery in Louisiana*, 44 S.U. L. Rev. 292, 314 (2017).
83 381 Search Warrants Directed to Facebook, Inc. v. New York County Dist. Attorney's Off., 132 A.D.3d 11, 13 (N.Y. App. Div. 2015).
84 *Id.* en la pág. 14.
85 *Id.*
86 *Id.*
87 *In the Matter of Search of Information Associated with Facebook Account Identified by the username Aaron. Alexis*, 21 F. Supp. 3d 1, 10 (D.D.C. 2013).
88 *Id.*

Por otra parte, en el caso de *Facebook, Inc. v. Superior Court*, el Tribunal Supremo de California dijo que cuando un usuario elige hacer sus publicaciones en las redes accesibles al público en general, éste ha hecho un consentimiento implícito.[89] A medida que se da este consentimiento, el proveedor de *Facebook* e *Instagram* debe cumplir con la divulgación de la información solicitada en el *subpoena* sin discreción a negarse. En el caso de *Monmouth-Ocean Hospital Service Corp*., el tribunal expresó que la S.C.A. era una ley para proteger la información privada, o aquella información en donde el usuario limita su privacidad, y que cuando un usuario convierte sus publicaciones inaccesibles al público en general, esta información está protegida bajo la ley.[90] Además, explicó que la privacidad no depende del número de amigos que un usuario tenga.[91] En este caso, la Corte citó el caso de *Crispin v. Christian Audigier Inc*., un caso civil en donde el demandado emitió *subpoenas* para los proveedores de *Facebook* solicitando todo tipo de información, tanto pública como privada, del demandante.[92] En este caso, el demandante solicitó impedir el *subpoena* argumentando que los proveedores estaban impedidos de desglosar.[93] El tribunal dijo que cualquier publicación que fuese pública no estaba protegida bajo la S.C.A., pero aquellas demarcadas privadas si lo estaban y no podían estar sujetas a un *subpoena* civil por una tercera parte que no fuera el Gobierno.[94]

B. Instagram

Instagram es una red social en donde las personas pueden publicar fotos o videos y compartirlos con sus seguidores o con un grupo selecto de amigos. Estos pueden ver, comentar y dar *me gusta* a las publicaciones compartidas por sus amigos en *Instagram*. Cualquier persona mayor de trece años puede crear una cuenta registrando una dirección de correo electrónico y seleccionando un nombre de usuario.[95]

> Cuando un usuario crea una cuenta en *Instagram*, la configuración predeterminada es que cualquiera que tenga acceso a la plataforma puede ver cualquier cosa que el usuario publique, a menos que este tome medidas afirmativas para cambiar la configuración de privacidad de su cuenta. El usuario tiene la opción de limitar el acceso de otros usuarios de *Instagram* a sus publicaciones. Si ese usuario de *Instagram* utiliza otras redes sociales como *Twitter* o *Facebook*, el usuario puede permitir que lo que el usuario publique bajo su cuenta de *Instagram*, también pueda ser publicado por las otras redes conectadas, y viceversa. Cabe destacar que no hay nada que evite que otro usuario pueda distribuir una publicación hecha en *Instagram* republicándola o tomando una captura de pantalla y publicándola en su propia cuenta.[96]

---

89 Facebook, Inc. v. Superior Court, 417 P.3d 725, 755 (2018).
90 Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 667 (D.N.J. 2013).
91 *Id.* en la pág. 668.
92 *Id.*
93 Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 969 (C.D. Cal. 2010).
94 *Id.* en la pág. 975.
95 People v. Sime, 85 N.Y.S. 3d 363, 367-68 (Crim. Ct. 2018).
96 *Id.*

Como fue mencionado anteriormente, las comunicaciones denominadas como privadas poseen la protección de la Cuarta Enmienda. Veamos cómo se ha desarrollado la jurisprudencia en cuanto a esta red social.

En el caso de *People v. Sime*, un individuo acusado de acoso agravado publicó fotos desnudas de su expareja.[97] El Tribunal autorizó una orden de registro y allanamiento para dos cuentas de *Instagram*: la del acusado y otra cuenta falsa a nombre de la víctima.[98] Ambas cuentas poseían una foto de la víctima al desnudo. El acusado cuestionó la legalidad del registro, argumentando que la orden: (1) carecía de causa probable; (2) era demasiada amplia y carecía de particularidad; (3) carecían de protocolos/limitaciones para minimizar la información que la policía podría revisar; (4) faltaban restricciones de fecha y hora; (5) no fue ejecutado dentro de diez días; (6) no fue ejecutado por agentes de policía, y (7) fue ejecutado fuera del estado de Nueva York.[99] El tribunal expuso que para analizar si la acción del Estado fue inconstitucional, habría que determinar si la persona tenía una expectativa razonable de intimidad en el lugar invadido —expectativa subjetiva— y si la sociedad reconocía la misma como razonable —expectativa objetiva—.[100] También expresó que quien tiene el peso de la prueba es el demandado.[101] El acusado en este caso no presentó prueba que estableciera que tomó pasos afirmativos para mantener privado su contenido de *Instagram*.[102] La Corte dictaminó que las órdenes emitidas por un juez se presumen válidas.[103]

Por otro lado, en el caso de *State v. Johnson*, la Policía de New Orleans obtuvo una orden de registro y allanamiento para la cuenta de *Instagram* de una víctima por asesinato.[104] El acusado de dicho asesinato sometió una moción de supresión de evidencia estableciendo que las órdenes de registro de la Policía carecían de causa probable.[105] El Tribunal de Distrito suprimió la evidencia.[106] El Estado apeló la decisión y el Tribunal de Apelaciones de Luisiana revisó al Tribunal de Distrito, estableciendo que este erró al suprimir la evidencia, puesto que el acusado no demostró tener una expectativa razonable de intimidad sobre la cuenta de la red social de la víctima, ni tampoco pudo demostrar que sufrió un daño por el registro ejecutado.[107] Expresó que el derecho a la intimidad que poseía la víctima sobre su cuenta de *Instagram* no se extendía al demandado, ya que la expectativa de privacidad que el acusado decía tener sobre esa cuenta de *Instagram* no era razonable.[108] Añadió que para el acusado poder argumentar que el registro era irrazonable, tenía que probar que se le violentó su expectativa razonable de intimidad, la cual no tenía pues la cuenta de *Instagram* no era suya.[109]

---

97 *Id.* en la pág. 366.
98 *Id.* en la pág. 367.
99 *Id.*
100 *Id.* en la pág. 369.
101 *Id.*
102 *Id.* en la pág. 370.
103 *Id.* en la pág. 371.
104 State v. Johnson, 276 So. 3d 1040, 1042 (La. Ct. App. 2019).
105 *Id.*
106 *Id.*
107 *Id.* en la pág. 1043.
108 *Id.*
109 *Id.*

A través de lo expuesto en esta parte sobre el tratamiento judicial a *Facebook* e *Instagram* —redes sociales de comunicación y promoción comercial— cabe entender que para que la protección de la Cuarta Enmienda cobije a las comunicaciones de los usuarios de estas redes, estos deben haber tomado medidas afirmativas dentro de la misma red, que subjetivamente le otorguen al usuario privacidad a sus comunicaciones.

C. TikTok

La misión de la plataforma *TikTok* es ser principal destino para videos móviles de formato corto. Su misión es inspirar la creatividad y brindar alegría.[110] Las estadísticas indican que *TikTok* cuenta actualmente con más de 689 millones de usuarios alrededor del mundo.[111] A diferencia de otras plataformas que se concentran en captar el estilo de vida del usuario, *TikTok* se destaca como una plataforma de entretenimiento. Generalmente, se graban videos de corto tiempo y se pueden compartir en otras redes sociales. La plataforma permite al usuario configurar las medidas de privacidad deseada en su cuenta, lo que podría cumplir con la acción afirmativa requerida por la Cuarta Enmienda para la expectativa razonable de intimidad subjetiva. Una cuenta catalogada como privada podrá aprobar o rechazar seguidores, así como permitir el acceso a ver su contenido y recibir mensajes solo de sus seguidores o personas específicas.[112]

Para obtener información privada de usuarios de *TikTok*, la agencia de ley debe proveer los documentos legales apropiados para obtener esa información como lo son: órdenes de registro y allanamientos, *subpoenas*, o someter una solicitud de emergencia.[113] *TikTok* proveerá la siguiente información: (1) información personal del usuario; (2) contenido de videos; (3) interacciones con otros usuarios tales como mensajes directos, videos entre usuarios y videos en vivo; (4) información de entrada y salida de la aplicación, y (5) contenido creado por el usuario.[114] Debido a que *TikTok* es relativamente nuevo, a la redacción de este escrito, no hay casos de referencia para analizar cómo las cortes se han expresado respecto a su expectativa de intimidad. Se podría entender que, al tener la aplicación configuraciones de privacidad disponibles dentro de sus medidas de seguridad, quedaría en manos del usuario su activación. De esta forma, la protección de la Cuarta Enmienda a la expectativa razonable de intimidad podría activarse en su manera subjetiva por las medidas afirmativas tomadas por el usuario.

La discusión de los tres tipos de redes sociales más usadas en el mundo, y la mirada a través de los estatutos vigentes dirigidos a la protección a la intimidad que brinda la Cuarta Enmienda de la Constitución de los Estados Unidos, lleva este escrito a su próximo y último tema: las propuestas de cambios al derecho actual.

---

110 *Nuestra misión,* TikTok, https://www.tiktok.com/about?lang=es (última visita 15 de marzo de 2022).

111 Maryam Mohsin, *10 TikTok Statistics That You Need to Know in 2021,* Oberlo (16 de febrero de 2021), https://www.oberlo.com/blog/tiktok-statistics.

112 *Ajustes de la cuenta,* TikTok, https://www.tiktok.com/safety/tools/your-account?lang=es&appLaunch=web (última visita 15 de marzo de 2022).

113 *TikTok Law Enforcement Guidelines,* TikTok (19 de abril de 2021), https://www.tiktok.com/legal/law-enforcement?lang=en.

114 *Id.*

III. Redes Sociales de Mensajería Instantánea Móvil

Las redes de mensajería instantánea móvil (en adelante, "*MIM apps*") —como *Messenger*, *WhatsApp,* y *Telegram*— permiten que los usuarios envíen en tiempo real mensajes de texto, mensajes de voz, fotos, videos y documentos a individuos o grupos de contactos. Estas plataformas también utilizan los servicios de VoIP por el cual permiten llamadas telefónicas y de video entre sus usuarios. Las cifras de usuarios de este tipo de redes son impresionantes. En el 2019, 2.56 mil millones de usuarios móviles utilizaron *MIM apps* para comunicarse, cifra que se estima crecerá a tres mil millones de usuarios para el año 2022.[115] Este tipo de red social se está convirtiendo rápidamente en el modo de comunicación preferido alrededor del mundo.[116]

Las redes de mensajería instantánea móvil se distinguen por haber adoptado las capacidades de cifrado,[117] incluyendo cifrado de fin a fin (en adelante, "E2EE", por sus siglas en inglés) en años recientes, incluyendo *WhatsApp*, quien desde abril del 2016 habilita este método de cifrado de forma predeterminada (*default*) para sus usuarios.[118]

A continuación, se discuten los tres *MIM apps* más usados y conocidos en Estados Unidos y Puerto Rico: *Messenger*, *WhatsApp*, y *Telegram*.

A. Una mirada general al cifrado y las aplicaciones de MIM

Es importante entender, aunque sea un tanto general, el proceso de cifrado para lograr comprender la privacidad y seguridad que ofrece ese tipo de tecnología cibernética. El proceso de cifrado revuelve o codifica el contenido de la comunicación digital, convirtiéndola así ilegible para cualquier persona o artefacto que no posea el código correcto de descifrado, o lo que se conoce como "la llave". Por ejemplo, con el cambio de +1 en el abecedario, la "A" sería "B", la "B" sería "C", y así sucesivamente. Así, la palabra "secreto" sería escrita "tfdsfup". Para descifrar el mensaje, el recipiente tendría que saber la llave, en este caso, el número de espacios que mover en el abecedario. La fuerza del cifrado es medida por el tamaño de su llave, ya que esta determina cuánto tiempo le tomaría a una computadora descodificar la data.

Los cifrados digitales actuales son mucho más complicados y técnicos que el ejemplo anterior, y fuera del alcance de lo que conlleva este escrito. Sin embargo, aunque sea en términos generales, resulta necesario explicar el cifrado digital actual para luego entender el análisis que los tribunales han tomado para enfrentar este tipo de red social. Justin Hurwitz lo explica de la siguiente manera:

> En términos bien generales, el cifrado es un proceso matemático por el cual información inteligible es transformada a una forma casi-ininteligible.

---

115 *Number of mobile phone messaging app users worldwide from 2018 to 2025*, Statista (15 de noviembre de 2022), https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide.

116 James A. Lewis et al., The Effect of Encryption on Lawful Access to Communications and Data 6 (2017).

117 Para propósitos de este escrito las palabras cifrado y encripción se utilizan como sinónimos, aunque pueden existir diferencias en el ámbito técnico de los términos.

118 Lewis et al., *supra* nota 116, en la pág. 6.

> Idealmente, la información encriptada es indistinguible del ruido aleatorio. Las ecuaciones usadas en esta transformación dependen de variables llamadas "llaves" —las llaves son nada más que números (típicamente bien largos). La característica que distingue estas ecuaciones es que no toman mucho tiempo en codificar o descodificar la información si conoces la llave, pero toma mucho tiempo descodificar información encriptada si no tienes la llave —y esta brecha entre cuánto tiempo tome descodificar la información con o sin la llave puede ser aumentada arbitrariamente utilizando llaves más largas. La razón por la cual toma tanto tiempo descodificar información encriptada sin la llave, es que un cifrado fuerte puede ser roto solo adivinando las llaves. El proceso de tratar llaves al azar para descodificar la información encriptada se conoce como un "ataque de fuerza bruta". Para poner este esfuerzo en perspectiva, un algoritmo moderno de cifrado le puede tomar a una computadora moderna un segundo para encriptar una pieza de información; descodificar esa información sin la llave podría fácilmente tomarle a la misma computadora un millón de veces más tiempo de lo que ha existido el universo. Por esta razón, los ataques mas exitosos al cifrado se aprovechan de errores en la codificación escrita por los programadores que implementan las ecuaciones de cifrado.[119]

Explicado el cifrado digital y sus capacidades, procedemos a conocer tres *MIM apps*: *Messenger*, *WhatsApp* y *Telegram*.

B. Messenger

Messenger es una aplicación gratis de MIM, creada por *Facebook* la cual permite enviar fotos, videos, grabaciones de voz y mensajes de grupo. El usuario puede utilizar *Messenger* para comunicarse tanto con sus "amigos" de *Facebook*, como con los contactos guardados directamente en su celular. A pesar de pertenecer a *Facebook*, *Messenger* es una aplicación aparte, aunque el sistema integrado de *Facebook* le permite acceder a *Messenger* sin necesariamente tener que descargar la aplicación al celular del usuario. La plataforma permite establecer conversaciones grupales con un máximo de cincuenta personas a la vez.[120]

La plataforma, al igual que las próximas por discutir, ofrece cifrado en sus conversaciones para fomentar y proteger la privacidad del usuario. *Messenger* también permite encriptar sus conversaciones con E2EE. Sin embargo, esto es una opción que el usuario debe habilitar. Otra función de seguridad que ofrece, aunque sólo a través de su aplicación, es la capacidad de tener "conversaciones secretas", en las cuales el usuario puede establecer la duración del mensaje antes de ser borrado. Por ejemplo, que sea borrado cinco segundos luego de haberlo leído/visto el receptor. Con esta opción *Messenger* incorpora la mensajería efímera a discutirse más adelante en la Parte IV de este escrito.

---

119 Hurwitz, *supra* nota 46, en la pág. 366 n.60 (*citando a* Ross Anderson, *Why Cryptosystems Fail*, 37 Comm. ACM 32 (1994) (traducción suplida).

120 Messenger, https://www.messenger.com (última visita 15 de marzo de 2022).

C. WhatsApp

WhatsApp es la *MIM app* más usada en el mundo.[121] Se distingue por ser la aplicación pionera de servicio de mensajería con cifrado integrado a todos sus clientes. En abril del 2016, *WhatsApp* comenzó a ofrecer E2EE a todos sus usuarios de manera automática, aumentando la seguridad de los mensajes enviados y recibidos por la aplicación. Esto, en el medio de la controversia que el cifrado en las telecomunicaciones ya se encontraba, luego de que el FBI demandara que *Apple* compartiera con la agencia de ley la "llave" para descifrar el celular del asesino en San Bernadino.[122]

La plataforma de *WhatsApp* permite conversaciones grupales de hasta 256 números de celular (contactos). Respecto al cifrado, *WhatsApp* no solo lo ofrece a sus usuarios de forma predeterminada, sino que no guarda la información de las llaves para descifrar las conversaciones en sus servidores. Al no tener la información disponible, en teoría, no importaría si se obtiene una orden de registro y allanamiento, pues la información simplemente no está disponible.

D. Telegram

De acuerdo a la propia página de *Telegram,* esta es un *MIM app* creado por dos hermanos rusos, quienes al igual que las oficinas generales de la compañía, están basados en Dubái.[123] A diferencia de *WhatsApp, Telegram* es mensajería basada en la nube con sincronización constante, a la cual el usuario se puede conectar desde cualquier dispositivo con acceso al internet .[124] En otras palabras, los usuarios no tienen que descargar la aplicación a su celular, aunque su número de teléfono celular es requerido para crear la cuenta del usuario.

Telegram permite conversaciones grupales con hasta 200,000 usuarios a la vez, al igual que ofrece la opción de crear un "canal" donde los mensajes llegarían a cualquier subscriptor del mismo, con capacidad ilimitada de personas.[125] La aplicación también permite "conversaciones secretas" con E2EE. Sin embargo, las conversaciones en la aplicación normal no son encriptadas con tecnología E2EE.[126] Esto significa que la aplicación guarda en sus servidores las llaves para descifrar los mensajes enviados con cifrado "regular". *Telegram* explica que, aunque esto parecería contradictorio a la seguridad –pues como vimos en la Primera Parte de este escrito, si el proveedor tiene la llave de descifrar en su poder, tendría que proveer el contenido del mensaje descifrado mediante una orden de registro y allanamiento. *Telegram* expresa que, aunque en efecto guarda la información de las llaves en sus servidores, estos se encuentran en diferentes países. Las llaves se dividen en dos o

---

121 Kemp, *supra* nota 60, en la pág. 95.
122 Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED (5 de abril de 2016), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.
123 *Telegram FAQ*, TELEGRAM, https://www.telegram.org/faq (última visita 15 de marzo de 2022).
124 *Id.*
125 *Id.*
126 *Id.*

más partes y estas partes nunca comparten servidores en un mismo país.[127] Además, según la compañía, *Telegram* podría compartir información con las autoridades si esta recibe una orden judicial que confirme que el usuario es sospechoso de terrorismo.[128]

E. Las aplicaciones de mensajería instantánea móvil, el cifrado y los tribunales

Como vimos en la Parte I de este escrito, el derecho a la privacidad de la Cuarta Enmienda es el derecho de los ciudadanos a mantener sus cuerpos y sus cosas "seguras" o que permanezcan en su propiedad, a menos que el registro sea razonable.[129] Aunque hay espacio para que el gobierno tenga acceso a las "personas, casas, documentos y efectos" de los ciudadanos, éste debe ser razonable.[130] En otras palabras, la corte vela primero por los intereses de la privacidad, y luego por los intereses del gobierno.[131]

Riley nos deja ver cómo el Tribunal Supremo de los Estados Unidos sigue este pensamiento, aun sabiendo, que en algunos momentos evidencia importante puede ser inaccesible: El Tribunal reconoce que su decisión "tendrá un impacto en la habilidad de las agencias de ley y orden de combatir el crimen" debido a que los "celulares se han convertido en herramientas importantes en la coordinación y comunicación entre miembros de entidades criminales, y podrían proveer información incriminatoria valiosa de criminales peligrosos. La privacidad tiene un costo".[132]

En el mismo caso, la Corte Suprema expresó que los celulares merecían protecciones adicionales de privacidad, y no pueden ser registrados sin una orden judicial específica ya que los celulares guardan el "todo de la vida privada del individuo", y no pedazos de información aislados como en tiempos pasados.[133] En el mundo, el ochenta y nueve por ciento de usuarios de Internet entre las edades de dieciséis a sesenta y cuatro años utilizan *MIM apps*, y la mayoría de estos lo hace a través de sus celulares.[134] Esto es una cifra alarmante.

El problema en el caso de las comunicaciones electrónicas es, irónicamente, la propia orden de registro. Una orden de registro que pide la información de una cuenta de un *MIM app* debería ser negada debido a su vaguedad. El peligro yace en que no habrá privacidad cuando la totalidad del contenido de la cuenta esté disponible al Estado para éste encontrar evidencia sin algún parámetro o restricción.

Algunas cortes, sin embargo, reconocen tal amenaza a la privacidad y han estado negando órdenes de registro generales para las comunicaciones encriptadas.[135] En un caso que incluía cuentas de varios proveedores, el Estado pidió órdenes de registro para distintas compañías, incluyendo el contenido de todos los correos electrónicos, MIMs, y *chat logs* de un sospechoso en un caso interestatal de propiedad robada.[136] La corte entendió

---

127 *Id.*
128 *Id.*
129 Const. EE. UU. enm. IV.
130 *Id.*
131 Gross, *supra* nota 55, en la pág. 78.
132 Riley v. California, 573 U.S. 373, 401 (2014) (traducción suplida).
133 *Id.* en la pág. 403 (traducción suplida).
134 Kemp, *supra* nota 60.
135 Gross, *supra* nota 55, en la pág. 85.
136 *In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts. No. 13-MJ-8163-JPO, 2013 WL 4647554, en la pág. *1 (D. Kan. 27 de agosto de 2013).

que las órdenes de registro eran muy abarcadoras ya que no incluían ningún límite a la información requerida y por esto violaban la Cuarta Enmienda.[137] La corte decidió que la orden de registro emitida, era análoga a una orden de registro pidiendo al correo que proveyera copias de todas las cartas, enviadas o recibidas, de una dirección en específico para que el gobierno pudiera abrir y leerlas todas y determinar si constituían fruto, evidencia o instrumentalidad de un crimen.[138]

En otro caso, la corte de distrito rechazó una petición de orden de registro, en la cual se solicitó registrar un celular incautado de manera legal, en parte porque la orden pedía el almacenamiento ilimitado de información encriptada.[139] En este caso, a la corte le preocupó que el Estado pudiera guardar la correspondencia completa enviada por *iMessage* –un *MIM app*– indefinidamente, la mayoría de la cual pudiese no tener causa probable al no tener conexión alguna con los crímenes investigados.[140]

Por otra parte, hay quienes proponen que el cifrado puede ser visto como una medida afirmativa necesaria para que se active la protección constitucional. Según discutido anteriormente, la protección de la Cuarta Enmienda requiere que el Estado obtenga una orden de registro y allanamiento cuando dicho registro podría infringir en la expectativa razonable de intimidad de la persona. Sin embargo, la expectativa tiene que ser razonable desde un punto de vista subjetivo y objetivo. Para cumplir con este requisito, la persona primero debe establecer que tiene una expectativa actual o subjetiva de intimidad, y segundo, que esa expectativa es una que la sociedad está preparada a reconocer como razonable.[141]

Como vimos en la Parte II, respecto a *Facebook* e *Instagram,* el Tribunal Supremo ha establecido también que los esfuerzos razonables que una persona toma para excluir a otros no son suficientes para que se active la protección de la Cuarta Enmienda; ya que es requisito fundamental que la expectativa razonable que subjetivamente tenga una persona, sea también honrada por la sociedad.[142]

Por el contrario, el Supremo ha sostenido que la Cuarta Enmienda provee protección al dueño de un contenedor que oculte su contenido a simple vista.[143] Por ejemplo, en *United States v. Chadwick*,[144] el Tribunal Supremo encontró que había expectativa razonable de intimidad en un *footlocker* cerrado bajo llave, aun cuando este se podía ver públicamente.[145] La protección en este caso no le aplicaba al *footlocker*, sino a su contenido.[146] Igualmente, en *Bond v. United* States,[147] la Corte determinó que el pasajero de una guagua tenía expectativa razonable de intimidad en su maleta "al usar un bulto opaco y ponerlo directamente encima de su asiento", aunque esta no se encontraba cerrada bajo llave o

---

137 *Id.* en la pág. 27.
138 *Id.* en la pág. 28.
139 *In re* Nextel Cellular Telephone, No. 14-MJ-8005-DJW, 2014 WL 2898262, en la pág. *1 (D. Kan. 26 de junio de 2014).
140 *Id.*
141 Katz v. United States, 389 U.S. 347, 361 (1967).
142 *Véase* Florida v. Riley, 488 U.S. 445 (1989).
143 United States v. Ross, 456 U.S. 798, 822-23 (1982).
144 United States v. Chadwick 433 U.S. 1 (1977).
145 *Id.* en la pág. 12.
146 *Id.* en las págs. 13-14.
147 Bond v. United States, 529 U.S. 334 (2000).

candado.[148] El Tribunal Supremo encontró que la opacidad del bulto era suficiente para satisfacer los requisitos de la expectativa razonable de intimidad, aún faltando el candado, ya que el bulto ocultaba su contenido de los que allí estaban. Al aplicar estos casos al contexto del cifrado y el mundo digital, podríamos llegar a la conclusión que estas comunicaciones están igualmente protegidas por la Cuarta Enmienda.

No es difícil entender que el único propósito del cifrado en *MIM apps* es prevenir el acceso no-autorizado a estas comunicaciones al convertirlos en ilegibles para todo aquel que no tenga la llave para descifrarlo. El hecho de que la información encriptada sea digital no debe disminuir la expectativa de privacidad. El cifrado es solo una herramienta de exclusión, el paso afirmativo para asegurar la privacidad: como el bulto en *Bond*,[149] o el *footlocker* en *Chadwick*.[150]

IV. Redes Sociales de Mensajería Efímera

Las redes sociales de mensajería efímera han sido desarrolladas con la intención de proveerle a sus usuarios una plataforma para compartir más información personal, sin alguna preocupación de que ese contenido sea permanente ya que es de naturaleza autodestructiva.[151] Las aplicaciones de mensajería efímera o "autodestructivas" se utilizan para enviar mensajes, fotos, videos u otras comunicaciones en un formato que automáticamente borra su contenido sin almacenamiento en ningún dispositivo. Aun cuando no ha sido resuelto por ningún tribunal, se entiende que la característica autodestructiva provee una expectativa de privacidad mayor al usuario, el cual entiende que ese contenido será borrado después de algunos minutos u horas. Las aplicaciones efímeras demuestran que hay una demanda en el mercado para herramientas de comunicación electrónica autodestructivas y que la privacidad por diseño es un modelo realista para las aplicaciones de redes sociales.[152]

A. Snapchat

Snapchat es una red social de rápido crecimiento y es mayormente popular entre personas de las edades entre trece y veinticuatro años. Sin embargo, ha ido ganando popularidad entre adultos de mayor edad últimamente.[153] Actualmente tiene aproximadamente 46 millones de subscriptores y es un ejemplo de una red social diseñada para la privacidad. Los servidores de *Snapchat* están diseñados para borrar el contenido de los mensajes enviados automáticamente después de haber sido vistos por todos los recipientes y borra automáticamente todos los mensajes no leídos en treinta días.[154]

---

148 *Id.* en la pág. 338 (traducción suplida).
149 *Id.*
150 *Chadwick*, 433 U.S. en la pág. 11.
151 Nicole Keefe, *Dance Like No One Is Watching, Post Like Everyone Is: The Accessibility of "Private" Social Media Content in Civil Litigation,* 19 Vand. J. Ent. & Tech. L. 1027, 1032 (2017).
152 Agnieszka McPeak, *Self-Destruct Apps: Spoliation by Design?*, 51 Akron L. Rev. 749, 753 (2017).
153 *Id.* en la pág. 750.
154 *Snapchat Support*, Snapchat, https://support.snapchat.com/en-US/a/when-are-snaps-chats-deleted (última visita 3 de abril de 2022).

Snapchat cuenta con medidas de privacidad que pueden ser editadas por cada usuario. El usuario puede elegir quién ve sus "snaps", quién le puede enviar mensajes, ver su historia, localización, entre otros. Aun cuando la aplicación está diseñada a autodestruir su contenido, nada impide que cualquier persona pueda grabar o guardar en su dispositivo la imagen o contenido recibido. Cada usuario tiene la expectativa de intimidad que escoge en sus ajustes de privacidad. Esto parecería implicar que las medidas afirmativas del contenido deben contar con las protecciones de la Cuarta Enmienda.

En el caso de *United States v. Peterson*,[155] el acusado fue entrevistado por dos oficiales de la policía con relación a la compra de unas armas frente a su casa. Los oficiales le pidieron permiso al acusado para entrar y conversar dentro de la casa, a lo cual el acusado accedió. La mayor parte de la entrevista fue hecha dentro de la residencia. Uno de los oficiales grabó el audio de la entrevista sin permiso del acusado. Cuando el acusado dio su versión de los hechos, el oficial le preguntó si tenía alguna conversación o mensaje en su celular que pudiese corroborar su versión. El acusado le mostró su celular y el oficial comenzó a grabar, con su propio celular, la pantalla del celular y los mensajes. Este expresó en voz alta que había visto mensajes sobre la compra de armas y escuchado conversaciones sobre drogas. Los oficiales le solicitaron al acusado firmar una autorización para que revisaran su celular. El acusado no estuvo dispuesto al principio, a lo que los oficiales contestaron que ya habían visto la evidencia, que podía firmar ahora o que eventualmente obtendrían una orden de registro. Eventualmente el acusado accedió, dio su contraseña y los oficiales se llevaron el celular. Luego de haber analizado el contenido de las conversaciones del celular, el fiscal obtuvo una orden de registro para la cuenta de *Snapchat* del acusado por estar relacionado a la compra de armas y sustancias controladas.

El acusado, a quien se le habían radicado varios cargos de posesión y distribución de drogas y armas, presentó una moción de supresión de evidencia argumentando que el gobierno violó sus derechos protegidos por la Cuarta Enmienda al: (1) entrar ilegalmente a su hogar, y (2) registrar y confiscar su celular ilegalmente. Como remedio, pidió que se suprimieran: (1) las declaraciones que le hizo a los agentes cuando entraron a su casa; (2) la evidencia que los agentes obtuvieron de su celular, y (3) cualquier evidencia adicional que las autoridades obtuvieron como fruto del registro a su celular, incluyendo toda la evidencia obtenida por una orden de registro posterior a su cuenta de *Snapchat*.

La corte decidió denegar la moción de supresión indicando que los agentes tenían causa probable para arrestar al acusado una vez vieron la evidencia en su celular, y que el consentimiento dado por él era suficiente para no estar en violación de las protecciones constitucionales de la Cuarta Enmienda. También añadió que la orden de registro para obtener la información de la cuenta de *Snapchat* del acusado en una fecha posterior fue razonable, ya que la obtención del contenido del celular fue con consentimiento.

---

155 United States v. Peterson, No. 3:18-CR-00049, 2018 U.S. Dist. WL 6061571 (D. Conn. 20 de noviembre de 2018).

V. Propuestas de Cambios

A. Nueva Legislación

Según expresado en la Parte II de este escrito, la Regla 41 de Procedimiento Criminal Federal, según enmendada en el 2009, es la que actualmente regula el proceso de registro y allanamientos a información almacenada electrónicamente. Esta regla tiene dos pasos a seguir. La primera parte es que debe completarse dentro de catorce días de haber sido autorizada, sin embargo, nada dice del tiempo que se tiene para revisar toda la información incautada ni el procedimiento para hacerlo, que es el segundo paso. Aun cuando estas órdenes de registro se rigen por la razonabilidad de la Cuarta Enmienda, son los oficiales de ley quienes tienen total discreción en ejecutar el segundo paso. Las comunicaciones electrónicas son fuentes valiosas de información. Algunas cortes y estudiosos del derecho han expresado preocupación con el procedimiento de registro de material electrónico ya que son prácticamente órdenes de registro generales, lo que socava las protecciones de la Cuarta Enmienda.[156] Por esto algunos magistrados han solicitado especificidades adicionales en sus ordenes tales como: (1) instituir limites de tiempo para completar el segundo paso; (2) mandato a devolver o borrar el material no responsivo, o (3) enumerar el protocolo de búsqueda a ser utilizado durante la ejecución.[157]

Aun cuando algunos magistrados han impuesto límites de tiempo en sus órdenes, otros se han alejado de esta limitación ya que la Cuarta Enmienda no lo exige como base para la razonabilidad [158]. El mandato de algunos magistrados a devolver o borrar el material no responsivo no ha sido bien acogido por las cortes. Algunas cortes han determinado que retener los materiales mientras los procedimientos están en curso, aun sin la intención de usarlos en alguna investigación ulterior, es razonable.[159] El mandato de enumerar el protocolo de búsqueda a ser utilizado goza de una lista de sugerencias que han sido contempladas. Las opciones son: (1) requerir un equipo independiente para que haga la revisión; (2) que los agentes utilicen una serie de términos específicos en la búsqueda, y (3) requerir que el proveedor haga una búsqueda inicial por términos específicos (*keywords*).[160] Todas estas alternativas limitan la cantidad de información inmaterial que se obtiene en los registros y que puede ser escudriñada por largos periodos de tiempo. Alguna de esta información contiene datos, conversaciones, vídeos, etc., de la persona implicada con terceros que de ninguna otra manera se hubiese obtenido.

En conclusión, según la tecnología continúa avanzando y la era digital trastoca todos los métodos de comunicación, es necesario implementar medidas que regulen y provean las protecciones constitucionales de la Cuarta Enmienda. La Regla 41 debe ser actualizada a la luz del proceso de los registros y allanamientos de información electrónica por parte del gobierno. La Cuarta Enmienda debe ser aplicada con fuerza para proteger la información de los ciudadanos americanos y asegurar la protección constitucional sobre regis-

156 Dennis, *supra* nota 24, en la pág. 2995.
157 *Id.* en la pág. 3002.
158 *Id.* en la pág. 3003.
159 *Id.* en la pág. 3005.
160 *Id.* (traducción suplida).

tros irrazonables. Aun cuando la Regla 41 continúe permitiendo que con sus dos pasos se descubra un universo de información en cualquier investigación, limitaciones afirmativas pueden asegurar que la Cuarta Enmienda se continúe protegiendo rigurosamente en la era digital. Los magistrados pueden asegurarse de que las órdenes de registro cumplan con la rigurosidad de las protecciones de la Cuarta Enmienda.[161]

B. Propuestas respecto al cifrado

A pesar de la presión que tiene el Congreso, de tanto los proveedores de estas nuevas tecnologías como de las agencias de ley y orden, este no ha tomado una posición contundente en la legalidad del cifrado. El incremento en el uso de esta tecnología, sobre todo del E2EE, debe cambiar el silencio por una expresión.

Sin embargo, el cifrado fuerte dificulta, y en algunos casos imposibilita, que el gobierno pueda obtener información de individuos, aun en casos donde se ha demostrado causa probable para exigir la información y una necesidad legítima de tener acceso a la misma.[162]

Estos son nuevos retos que no han sido considerados por el Congreso. Los tipos de proveedores de servicios cubiertos bajo la E.C.P.A. y C.A.L.E.A. no habían ofrecido anteriormente las capacidades del E2EE; a lo sumo, proveían almacenamiento para la información cifrada por un tercero. Esto representa un cambio más dramático en la relación entre los derechos de los individuos y las necesidades del Estado que cualquier otro cambio anterior en la tecnología de las comunicaciones.

En su artículo, Shannon Gross menciona:

> Las agencias de ley y orden argumentan que el cifrado pudiera impedir el descubrimiento de un plan terrorista, de explotación infantil, o de trasiego de drogas, entre otros crímenes. Dicen tener preocupaciones de seguridad como la razón para justificar la cooperación de las compañías de cifrado. Sin embargo, hay otro interés de seguridad en el que el cifrado no estorba, sino que ayuda: seguridad digital. El cifrado mantiene las comunicaciones entre las personas y su información personal privadas, previniendo de esta manera el *hacking* y otros riesgos a la privacidad digital. Al abrirle el sistema digital de cifrado al Estado, probablemente se le abriría también el sistema a *hackers* interesados en robar la información personal de los ciudadanos, causando así más crímenes, aun cuando las agencias tratan de prevenirlo.[163]

Las cortes tienen dos opciones si decidieran tratar los mensajes encriptados análogamente a jurisprudencia anterior. Pueden tratar los mensajes como una caja asegurada con candado (con expectativa razonable de intimidad) o como un secreto o comunicación codificada (sin expectativa razonable de intimidad). También podrían crear un nuevo entendimiento en vez de forzar la tecnología actual dentro de leyes antiguas.

---

161 Reid Day, *supra* nota 43, en la pág. 494.
162 Hurwitz, *supra* nota 46, en las págs. 372-73.
163 Gross, *supra* nota 55, en la pág. 91 (traducción suplida).

Conclusión

"Sin importar lo que la Corte Suprema decida hacer con las redes sociales en el internet, solo los más ignorantes o crédulos piensan que lo que publiquen en el internet es o permanece privado".[164]

Hoy en día las redes sociales son la fuente de mayor filtración de información personal diaria. En esta era tecnológica que vivimos, las redes sociales son una herramienta de comunicación, intercambio de información y entretenimiento que al igual sirven de instrumento para la búsqueda de la verdad y la justicia.

Los detalles de la mejor manera de proceder con la ejecución de las órdenes de registro y allanamiento se han dejado a discreción de los oficiales de ley y orden al carecer legislación que atienda este tipo de tecnologías directamente. Sin embargo, el Tribunal Supremo de los Estados Unidos ha definido lo que es un registro y allanamiento razonable, y han demostrado a través de las decisiones discutidas en este escrito, que el derecho a la intimidad se debe atender seriamente, y no puede ser desatendido a favor de la seguridad pública.

Esto es un área del derecho en crecimiento y como no hay unas guías en específico que los oficiales deban seguir, se ha atendido caso a caso y los tribunales, como hemos demostrado, han dictaminado opiniones variantes de cómo se debe proceder ante la difícil tarea de aplicar la Cuarta Enmienda a la era digital. Lo cierto es que se debe atender esta ambigüedad en el proceso, puesto que el derecho a la privacidad de los usuarios está en juego.[165]

Como este artículo ha demostrado, las leyes proveedoras de protección para las comunicaciones electrónicas son anticuadas y la jurisprudencia está dividida a través de la nación, sin que reluzca alguna tendencia real entre las cortes. Más importante aún, este artículo expresa una esperanza de que existan preocupaciones comunes a ambos lados de la balanza. La tecnología siempre va avanzando y es importante que de igual manera lo haga el Derecho. Vivimos una era de tecnología dinámica y cambiante, por lo que es necesario utilizar las herramientas que la tecnología nos provee para mejorar el ordenamiento jurídico puertorriqueño.[166] Dentro de los próximos años, el Congreso tendrá que considerar y adoptar una legislación que enfrente las preocupaciones de privacidad en las redes sociales y sobre los métodos de cifrado.

---

164 Tapia v. City of Albuquerque, 10 F. Supp. 3d 1323, 1388 (D.N.M. 2014) (traducción suplida).
165 Smith, *supra* nota 20, en las págs. 128-31.
166 Niodra Antoinette Quiñones Ufret, *La identificación del sospechoso mediante las redes sociales bajo la doctrina del "show up"*, 58 Rev. D.P. 89, 89-93 (2018).