ESTADO LIBRE ASOCIADO DE PUERTO RICO
COMISIÓN DE DERECHOS CIVILES

Apartado 192338
San Juan, PR 00919-2338
787.764.8686 | TTY: 787.765.9360
Fax: 787.250.1756
www.cdc.pr.gov

Informe de la Comisión de Derechos Civiles

Vigilancia Gubernamental y Protesta Pública en Puerto Rico: Análisis de prácticas de vigilancia por la Policía de Puerto Rico durante las manifestaciones del 1ro de mayo de 2017

Querella Núm. 2017-04-16861

24 de abril de 2019

ESTADO LIBRE ASOCIADO DE PUERTO RICO
COMISIÓN DE DERECHOS CIVILES

Apartado 192338
San Juan, PR 00919-2338
787.764.8686 | TTY: 787.765.9360
Fax: 787.250.1756
www.cdc.pr.gov

Informe de la Comisión de Derechos Civiles

Vigilancia Gubernamental y Protesta Pública en Puerto Rico: Análisis de prácticas de vigilancia por la Policía de Puerto Rico durante las manifestaciones del 1ro de mayo de 2017

Querella Núm. 2017-04-16861

ESTADO LIBRE ASOCIADO DE PUERTO RICO
COMISIÓN DE DERECHOS CIVILES

Apartado 192338
San Juan, PR 00919-2338
787.764.8686 | TTY: 787.765.9360
Fax: 787.250.1756
www.cdc.pr.gov

Informe de la Comisión de Derechos Civiles

Vigilancia Gubernamental y Protesta Pública en Puerto Rico: Análisis de prácticas de vigilancia por la Policía de Puerto Rico durante las manifestaciones del 1ro de mayo de 2017

Querella Núm. 2017-04-16861

Introducción

En una comunidad con aspiraciones democráticas, como la nuestra, los derechos políticos son indispensables. Los derechos de libertad de expresión y asociación, así como el derecho a la intimidad y al anonimato en la esfera privada y pública son precondiciones necesarias—aunque no suficientes—para la interacción social democrática y para la vida política de una sociedad pluralista. Sin estas protecciones no hay posibilidad de un ambiente discursivo público que provea oportunidades de auto reflexión sobre nuestro estado de situación colectiva y, con ello, la posibilidad de imaginar nuevas y más justas formas de vida. Sin un discurso público vigoroso, materializado con la palabra en privado y en público (entre conocidos y desconocidos) y manifestado con acciones concretas frente a otras y otros a través de la protesta y del reclamo potente al gobierno, no es posible hablar de un estado democrático legítimo. Mucha de esta conducta (aunque no toda) ocurre a la vista de todas y todos, además de que la vigilancia gubernamental constante de prácticas discursivas amenaza estas posibilidades democráticas. Un ambiente discursivo supervisado y vigilado—y sin controles a la supervisión que pueda hacerse para ciertos fines legítimos—socava el

AVENIDA PONCE DE LEÓN #416, EDIFICIO UNION PLAZA, OFICINA 901, HATO REY, PUERTO RICO 00918

sentido de seguridad que el público necesita para ejercer sus derechos democráticos sin temor a la represalia.

Las tecnologías de información contemporáneas hacen posible ciertas formas de interacción social digitalmente interconectadas que eran imposibles de imaginar en el siglo XX, cuando la Constitución de Puerto Rico fue forjada. En un sentido importante, estas tecnologías han transformado profundamente la ecología discursiva: si bien potencian la comunicación humana distribuida globalmente y disminuyen los costos de coordinación para la acción colectiva, al mismo tiempo presentan retos sociales importantes, entre los cuales se encuentran mayores posibilidades de vigilancia ubicua. Las mismas tecnologías que magnifican el alcance de las voces de personas, aumentan también las oportunidades de vigilancia de forma más eficiente y, por ende, más preocupante. La necesidad de controles a la acción investigativa del Estado es, más que nunca, indispensable.

Si bien la práctica de confeccionar carpetas contra personas por razones políticas en Puerto Rico durante el siglo XX fue devastadora, "[s]e trataba, en términos relativos, de un sistema muy ineficiente" ya que el esfuerzo requería una cantidad impresionante de recursos, logística organizativa, espacio físico y mano de obra. En este sentido, "[a]ún en un ambiente de persecución rampante, el anonimato y la intimidad seguían siendo posibles a través de las limitaciones reales del sistema". Hoy día, sin embargo, "los métodos tecnológicos disponibles…hacen que los mecanismos de orden público

sean exponencialmente más eficientes, eliminando muchas de las protecciones *de facto* que los métodos no digitales proveían."[1]

En este informe, la Comisión de Derechos Civiles evalúa la infraestructura investigativa del gobierno de Puerto Rico. Nuestra intervención emana de una querella presentada ante esta Comisión días antes de las actividades de protesta multitudinarias en Puerto Rico el 1 de mayo de 2017, como reacción a expresiones emitidas por la entonces Superintendente de la Policía de Puerto Rico, Coronela Michelle Hernández de Fraley. Estas expresiones fueron a los efectos de que la Policía monitoreaba las redes sociales de las y los manifestantes, en anticipo a las actividades del 1 de mayo. En la querella se alegó que estas expresiones eran una práctica de espionaje digital, tan repudiable e ilegal como el carpeteo sufrido por cientos de miles de independentistas en el pasado.

La querella, por tanto, planteó la necesidad de examinar las prácticas y políticas de las agencias de ley y orden de Puerto Rico que inciden sobre la supervisión de la actividad de la protesta pública en el país, así como el marco legal, reglamentario y constitucional pertinente. A la luz de esta encomienda, la Comisión de Derechos Civiles realizó una investigación que consistió de tres vistas públicas con participación de personas de la comunidad y funcionarios públicos; múltiples requerimientos de información a la Policía de Puerto Rico; un requerimiento de información a un proveedor de servicios de Internet; una Inspección Ocular al Centro de Recopilación, Análisis, Diseminación de Inteligencia Criminal (C.R.A.D.I.C.) y a la División de

[1] Hiram Meléndez Juarbe, *La Constitución en Ceros y Unos: Un Acercamiento Digital al Derecho a la Intimidad y la Seguridad Pública,*77 Rev. Jur. UPR 45 (2008).

Crímenes Cibernéticos de la Policía, así como reuniones con entidades pertinentes y el examen de cientos de documentos, unidos al correspondiente estudio del derecho puertorriqueño y de Estados Unidos aplicable. Este examen se realizó tomando en cuenta como punto de partida la siguiente interrogante:

> Si las prácticas y políticas de la Policía de Puerto Rico relacionadas con la vigilancia y el monitoreo en el contexto de actividades de protesta pública violentan los derechos de libertad de expresión, asociación e intimidad de las puertorriqueñas y los puertorriqueños.

Al abordar esta pregunta, la Comisión de Derechos Civiles consideró, a su vez, las siguientes interrogantes:

1. ¿Qué controles institucionales existen para evitar el riesgo de que los funcionarios públicos abusen de las herramientas investigativas a su disposición para incurrir en prácticas de vigilancia que constituyan una violación a los derechos constitucionales?

2. Como parte de sus actividades de vigilancia a través de la internet, ¿qué mecanismos utilizan las agencias de ley y orden en Puerto Rico para solicitar información personal que recopilan entidades privadas sobre sus clientes o usuarios (como es el caso de las redes sociales o los Proveedores de Servicios de Internet)? Asimismo, y relacionado, ¿son estas prácticas consistentes con el ordenamiento legal y constitucional vigente?

3. ¿Qué tecnologías de información—y cuáles son los protocolos y los controles asociados a ellas—que utiliza la Policía de Puerto Rico para realizar actividades de vigilancia para el contexto de las protestas públicas? ¿Qué preocupaciones de naturaleza legal y constitucional generan estas tecnologías de la información e investigación?

Tras el examen de la información recopilada en esta investigación, la Comisión de Derechos Civiles en este informe emite diversas conclusiones y recomendaciones que operan a diferentes niveles y atienden aspectos de las prácticas bajo evaluación. En algunos casos se ofrecen recomendaciones sobre prácticas que presentan visos claros

de inconstitucionalidad, en otros sobre prácticas que resulta imperativo mejorar, independientemente de si son inconstitucionales o no. Estas conclusiones y recomendaciones aparecen a través de este informe, y se recapitulan en las secciiones finales.

La Comisión de Derechos Civiles fue creada en el 1965 y tiene entre sus funciones la protección de los derechos humanos y monitorear el estricto cumplimiento de las leyes que los amparan.[2] Además, realiza estudios e investigaciones sobre la vigencia de los derechos humanos en Puerto Rico y atiende querellas presentadas a su consideración.

La Comisión de Derechos Civiles cuenta con independencia de criterio, es una institución *sui generis* con autoridad para evaluar las políticas y prácticas de las agencias gubernamentales desde la perspectiva de los derechos humanos reconocidos en la Constitución de Puerto Rico y en los instrumentos internacionales. Por ello, sus Comisionadas y Comisionados provienen de la sociedad civil y cuentan con *expertise* en el campo de los derechos humanos, cuentan con nombramientos a término y ejercen sus funciones *ad honorem*.

Los informes de la Comisión han sido refrendados y citados con deferencia por el Tribunal Supremo de Puerto Rico en los casos de: *Leyra v. Aristud*[3], en torno a la intervención policial; *Noriega v. Gobernador*[4], relacionado con la práctica del carpeteo; *El Vocero v. ELA*[5], tocante a la libertad de prensa y *De Castro, Ombudsman v.*

[2] Ley Núm. 102 de 28 de junio de 1965, 1 L.P.R.A 151.
[3] 132 D.P.R. 376, 489 (1993).
[4] 130 D.P.R. 919 (1992).
[5] 131 D.P.R. 356 (1992).

Cordero[6], sobre las investigaciones administrativas. Además, han servido de base para el desarrollo de legislación y políticas públicas, por ejemplo, la ley orgánica de la oficina especializada sobre asuntos de las mujeres, hoy día la Oficina de la Procuradora de las Mujeres.

En el ejercicio de estas funciones, la Comisión atendió la querella presentada[7] y emite este informe.

I. Trámite procesal

El 26 de abril de 2017, el Representante a la Cámara, Denis Márquez Lebrón y el Senador Juan Dalmau presentaron una querella ante la Comisión en la que solicitaron que se investigaran las expresiones que reseñó la prensa ese mismo día, de la entonces Superintendente de la Policía de Puerto Rico, Coronela Michelle Hernández de Fraley. Las expresiones de la Superintendente fueron a los efectos de que monitoreaba las redes sociales de personas, en anticipo a la marcha del 1ero de mayo de 2017. Como se detallará más adelante, alegaron los querellantes que estas expresiones, sumadas a las admisiones de la Superintendente de que se estaban tomando videos, fotografías y archivando expresiones realizadas en las redes sociales a personas y organizaciones que anticipaban participar de protestas legítimas contra las policitas económicas y laborales de la actual administración, constituían una práctica de espionaje cibernético, tan repudiable e ilegal como el carpeteo sufrido por cientos de miles de independentistas en el pasado.

---

[6] 130 D.P.R. 376, 399 (1992).
[7] Querella Núm. 2017-04-16861.

La consideración de la querella estuvo a cargo de la Lcda. Georgina Candal Segurola, Presidenta de la Comisión de Derechos Civiles; de la Dra. Esther Vicente, Vicepresidenta; del Dr. Hiram Meléndez Juarbe, Comisionado; y de la Lcda. Patricia Otón Olivieri, Comisionada. De conformidad con la legislación aplicable[8], y con el *Reglamento para el Procesamiento de Solicitudes de Servicios y Querellas de la Comisión de Derechos Civiles*[9], se convocaron vistas para atender el asunto planteado en la querella y se cursaron requerimientos de información.

Hacemos constar que, mediante la Ley Núm. 20 de 10 de abril de 2017, conocida como la Ley del Departamento de Seguridad Pública de Puerto Rico, se creó el Departamento de Seguridad Pública, a cargo de un Secretario. En virtud de esta Ley, la Policía de Puerto Rico pasa a ser el Negociado de la Policía de Puerto Rico, a cargo de un Comisionado, antes Superintendente, ahora consolidado bajo este. Toda vez que la vigencia de dicha ley comenzó 180 días luego de su aprobación,[10] al momento de los eventos del 1 de mayo de 2017, el cargo relevante era el de Superintendente. A través de este informe nos referiremos en general a la Policía de Puerto Rico o PPR, cuando se trate de una mirada retroactiva; asimismo, nos referiremos al Negociado de la Policía de Puerto Rico, NPPR, cuando el contexto lo requiera, para dar cuenta del cambio en estructura.

[8] 1 L.P.R.A. 153.
[9] Aprobado en el 2015.
[10] Artículo 9.07 de la Ley Núm. 20 de 10 de abril de 2017.

II. Querella Presentada y Controversias ante la Comisión de Derechos Civiles

Mediante carta enviada el 26 de abril de 2017, el Representante Denis Márquez Lebrón, solicitó a la Comisión de Derechos Civiles que investigara unas expresiones hechas en la prensa, por la Superintendente de la Policía, Michelle Hernández de Fraley. Según la carta, la funcionaria manifestó que la Policía de Puerto Rico "monitorea las redes sociales de los manifestantes, en anticipo a la marcha del próximo 1 de mayo". Además, se alegó en la querella que esta admitió que "se están tomando videos, fotografías, y archivando expresiones realizadas en las redes sociales a personas u organizaciones que anticipan participar de protestas legítimas en contra las políticas económicas y laborales de la actual administración".

El querellante planteó que los actos señalados constituían una violación a los derechos de los ciudadanos contrarios a las determinaciones hechas por el Tribunal Supremo de Puerto Rico, en el caso *Noriega Rodríguez v. Hernández Colón*, 122 D.P.R. 650 (1988), en el que se estableció que: "...la práctica de levantar expedientes, carpetas, listas, ficheros, etc. de personas, agrupaciones, y organizaciones única y exclusivamente por motivo de las creencias políticas e ideologías de estos sin que tenga evidencia real que vincula a esas personas con la comisión o intento de comisión de un delito es, ilegal e inconstitucional por infringir los derechos de libertad de palabra, de asociación, de privacidad y por constituir ello una afrenta a la dignidad del ser humano". Además, solicitó se considerara el *injunction* de carácter permanente concedido en contra del Estado para que cesara y desistiera de la práctica de "carpeteo" y ordenó la

entrega de expedientes confeccionados al demandante y a toda persona en su situación, entre otros remedios.[11]

En relación a la querella presentada por el Representante, se han revisado varios artículos de periódico publicados por Metro PR, Primera Hora y El Vocero. Los artículos mencionados contienen la siguiente información sobre expresiones realizadas por la entonces Superintendente el 26 de abril de 2017, a días de celebrarse una protesta pública masiva pautada para el 1 de mayo de ese año:

> La Superintendenta de la Policía, Michelle Hernández de Fraley, dio a conocer hoy que monitorean las redes sociales para preparar sus planes de trabajo de cara a las manifestaciones. La División de Crímenes Cibernéticos es la encargada de verificar las redes sociales diariamente.
>
> > "Estamos monitoreando las redes sociales tenemos acceso a lo que se ha manifestado de las diferentes organizaciones y basado en eso desde el viernes pasado hemos contemplado nuestro plan de trabajo que no es nuestro solo, sino que también reconoce a otras organizaciones estatales que van a estar con nosotros antes, durante y después para trabajar todo lo que ocurra relacionado al 1 de mayo".
>
> Indicó que tienen acceso a Facebook donde "todo el mundo postea sus intenciones y nosotros monitoreamos esas intenciones y corroboramos que las intenciones son más que palabras para entonces eso nos pone en una postura".[12]
>
> ***
>
> La superintendente de la Policía, Michelle Hernández de Fraley, dijo hoy que el cuerpo que dirige se está preparando para el manejo de la protesta

[11] Cabe destacar que en el 1970 la Comisión de Derechos Civiles examinó la recopilación de nombres de personas a base de sus ideas políticas y afirmó que esto constituía "una práctica peligrosa y a veces ilegal de investigación policial sobre la conducta y actividades de individuos y grupos. Estas y cualesquiera otras formas que se utilicen para recoger información, sólo se justifican cuando guardan una relación próxima, directa o circunstancial, con una posible actividad delictiva". La Vigilancia e Investigación Policíaca y los Derechos Civiles (18 de febrero de 1970), 1970, CDC 014, 2 Der. Civ. 27, 54 (1973).

[12] Meléndez, Lyanne, *Policía verifica redes sociales de los manifestantes,* Metro PR, 26 de abril de 2017, https://www.metro.pr/pr/noticias/2017/04/26/policia-verifica-redes-sociales-manifestantes.html

del 1 de mayo, monitoreando las redes sociales para anticipar cualquier amenaza.

> "Todo el mundo postea sus intenciones y nosotros monitoreamos esas intenciones y corroboramos que las intenciones son más que palabras. Eso entonces nos pone en una postura", abundó luego de informar que están monitoreando las redes sociales en anticipo al 1 de mayo.

Hernández de Fraley confirmó a preguntas de EL VOCERO que la información recopilada por encubiertos durante las manifestaciones es compartida con agencias federales a través del Centro de Fusión.[13]

***

La superintendente de la Policía, Michelle Hernández de Fraley, dijo ayer que el cuerpo que dirige se está preparando para atender el paro nacional convocado para el 1 de mayo, monitoreando las redes sociales para anticipar las "intenciones" de los manifestantes, mientras admitió que se comparten estas informaciones con las autoridades federales.[14]

***

La superintendenta de la Policía, Michel Hernández de Fraley, confirmó hoy que monitorean las redes sociales de grupos e individuos que han acudido a manifestaciones o han convocado al paro nacional el 1 de mayo. Hernández dijo que, como todo el mundo, tienen acceso a Facebook y otras redes y lo están utilizando para trazar su plan para las próximas protestas.

> "Todo el mundo postea sus intenciones y nosotros monitoreamos esas intenciones y corroboramos que las intenciones son más que palabras", aseguró a preguntas de la prensa.[15]

---

[13] Quintero, Laura M., *Policía monitorea redes sociales de los manifestantes,* El Vocero, 26 de abril de 2017, http://elvocero.com/policia-monitorea-redes-sociales-de-manifestantes/

[14] Quintero, Laura M., *Lista la Policía para la protesta del lunes,* El Vocero, 27 de abril de 2017, http://elvocero.com/lista-la-policia-para-la-protesta-del-lunes/

[15] Colón, María de los M., *Policía le tiene el ojo echa'o a las redes sociales,* Primera Hora, 26 de abril de 2017, http://www.primerahora.com/noticias/gobiernompolitica/nota/policialetieneelojoechaoalasredessociales-1220329/)

El jueves 25 de mayo de 2017, la Comisión de Derechos Civiles celebró la primera audiencia pública de este caso. En la audiencia, comparecieron a deponer como querellantes el Representante Denis Márquez Lebrón y el Senador Juan Dalmau Ramírez, ambos del Partido Independentista Puertorriqueño. Estos sometieron sendas ponencias y contestaron las preguntas de las Comisionadas. Según el licenciado Márquez, ni el Tribunal Supremo de Puerto Rico ni el de Estados Unidos ha determinado que la información publicada en las redes sociales es inequívocamente pública y por ende accesible al Estado para cualquier fin. Aunque entiende que es posible que alguna expectativa de intimidad se pueda perder sobre ciertos asuntos, ello no significa que sean tan fácilmente renunciables el derecho a la intimidad, así como el derecho a la libre expresión y asociación. Además, adujo que el hecho de que cualquier información pueda catalogarse como pública "no implica que el Estado pueda recopilarla sin ninguna restricción basándose únicamente en las ideas políticas y sociales de la persona afectada, o como castigo por el ejercicio de un derecho constitucional". El Representante puntualizó además, que entiende que la práctica de monitoreo electrónico es una continuación de la práctica de "carpeteo" vedada por nuestro Tribunal Supremo y que la entrega de las carpetas no significa que la Policía de Puerto Rico haya cambiado sus prácticas o políticas en torno al tema.

Por su parte, el Senador Juan Dalmau Ramírez indicó que entiende que se han violentado los derechos de asociación, expresión, propia imagen e intimidad. Este llamó la atención de la Comisión a los estándares y normas sobre derechos humanos transgredidas por la práctica denunciada. Entre estas, la Declaración Americana de los Derechos y Deberes del Hombre, de la Organización de Estados Americanos y la

Declaración Universal de Derechos Humanos de la Asamblea General de las Naciones Unidas. Ambos documentos establecen como libertades protegidas el derecho a la libertad de investigación, de opinión, de expresión y difusión del pensamiento por cualquier medio, el derecho de toda persona a asociarse con otras para promover y ejercer intereses legítimos de orden político, económico, religioso, social y cultural; y el derecho a la libertad de pensamiento, de conciencia y de religión. Este derecho incluye "el no ser molestado a causa de sus opiniones...y el de difundirlas...por cualquier medio de expresión", puntualizó.

El Senador expresó además que la Comisión debe investigar con detenimiento si la Policía de Puerto Rico ha desarrollado un nuevo instrumento que constituye una violación de derechos constitucionales, para vigilar el comportamiento social de las personas y no su actividad criminal. Finalmente manifestó preocupación sobre las expresiones de la Superintendente a los fines de que estas puedan malinterpretarse por los policías a los fines de "que no hay reglas que los limiten" y de que tienen permiso para intervenir con quienes se manifiestan y expresan opiniones disidentes.

Como parte de sus respectivas ponencias, los querellantes solicitaron a la Comisión que:

1. Se investiguen los procesos por medio de los cuales la Policía de Puerto Rico hace monitoreo de redes sociales.

2. Requiera toda la información que sea necesaria a los fines de determinar si la Policía de Puerto Rico ha generado perfiles de personas con contenidos relativos a sus actividades de expresión pública.

3. Constate si la Policía de Puerto Rico mantiene acervo de videos o fotografías de protestas sin que estas sean objeto de alguna investigación criminal.

4. Indague sobre:

    a. Si la Policía ha levantado expedientes a personas o entidades
    b. Cómo se conserva la información recopilada
    c. Qué criterios se utilizan para determinar a quién y cómo se monitorea a alguien.
    d. Qué redes sociales se están monitoreando
    e. Cómo el Estado tuvo acceso a dichas cuentas
    f. Si hay entidades públicas o privadas compartiendo información que aparece en las redes sociales
    g. Si existe relación entre agencias de gobierno para compartir esa información
    h. Si medió una orden judicial basada en causa probable para cualquier solicitud de esa naturaleza
    i. Si se han centrado investigaciones criminales a base de dicha actividad de monitoreo
    j. Qué ha pasado con las fotografías y los videos que la Policía de Puerto Rico toma y si se ha destruido información digital

Finalmente, los funcionarios solicitaron que la Comisión haga un análisis sobre los derechos que esta práctica infringe. Puntualizaron que la investigación de la Comisión y su posterior publicación sería utilizada para tomar acciones legislativas puntuales.

III. Resumen de las gestiones realizadas

Durante el periodo de investigación de la presente Querella se llevaron a cabo las siguientes gestiones:

1. **25 de mayo de 2017** – Primera Audiencia Pública llevada a cabo en la Comisión de Derechos Civiles, donde los querellantes exponen sus reclamos y el contenido de su querella.

2. **30 de mayo de 2017** – Primer Requerimiento de Información "Habeas Data" a la Policía de Puerto Rico sobre el monitoreo de redes sociales, cómo y de qué manera se utilizan, además de los videos, fotos y listas de personas señaladas por participar en la manifestación del 1 de mayo de 2017.
3. **5 de julio de 2017** – Segunda Audiencia Pública llevada a cabo en la Comisión de Derechos Civiles, a la cual comparecieron la parte querellada, la Superintendente de la Policía, Cor. Michelle Hernández de Fraley y otro personal de la Policía, además del entonces Director de la Unidad Investigativa de Crímenes Cibernéticos del Departamento de Justicia, el Fiscal Rafael Sosa.
4. **3 de noviembre de 2017** – Segundo Requerimiento de Información "Habeas Data" sobre los protocolos para compartir información con el Negociado Federal de Investigaciones, sobre la Superintendencia Auxiliar de Investigaciones Criminales (S.A.I.C), adiestramientos al personal de la Policía que acude a manifestaciones para realizar grabaciones, información sobre la Sección de Análisis de Inteligencia Criminal (C.R.A.D.I.C.) e información acerca de la Sección Técnica de Grabaciones (UTG), entre otros.
5. **30 de noviembre de 2017** – Se emite un "Subpoena Duces Tecum" como seguimiento al segundo requerimiento enviado el 3 de noviembre de 2017 del cual no se había obtenido respuesta. El Subpoena requería además una lista de información, documentos y preguntas a contestar por parte de la Policía de Puerto Rico.

6. **5 de diciembre de 2017** – Requerimiento al Departamento de Justicia para solicitar información sobre las guías para el uso de evidencia electrónica, proveedores de servicios de Internet utilizados, entre otros
7. **8 de diciembre de 2017** – Reunión del Comisionado Meléndez Juarbe con el Director de la Sección de Vigilancia Doméstica del Electronic Privacy Information Center, para discutir posibles acercamientos a la problemática bajo análisis.
8. **16 de febrero de 2018** – Inspección Ocular en el Cuartel General de la Policía de Puerto Rico, donde se encuentran las oficinas de C.R.A.D.I.C. y la División de Crímenes Cibernéticos, áreas las cuales la Comisión tuvo la oportunidad de visitar y también entrevistar al personal.
9. **15 de marzo de 2018** - Reunión con el Sr. Arnaldo Claudio, Asesor Técnico de Cumplimiento para el caso judicial federal bajo el cual la Policía está requerida a reformar sus prácticas y políticas. Esta reunión se suscitó para dialogar e intercambiar impresiones sobre los hallazgos del informe preparado por la Oficina del Asesor Técnico sobre las manifestaciones del 1 de mayo de 2017 en Hato Rey y otras demostraciones.
10. **9 de abril del 2018** – Tercer Requerimiento de Información "Habeas Data" a la Policía de Puerto Rico. Entre otras preguntas de seguimiento, se solicitó información sobre los hallazgos del informe recién publicado por la Oficina del Asesor Técnico de la Policía en relación a los eventos del 1 de mayo de 2017.
11. **11 de abril de 2018** – Tercera Audiencia Pública llevada a cabo en la Comisión de Derechos Civiles, donde comparecen el Representante Denis Márquez

Lebrón, el Sr. Ricardo Oliveros, y la Lcda. Mariana Nogales, acompañada de la Lcda. Nicole Díaz. Expusieron sus experiencias con la Policía de Puerto Rico en manifestaciones públicas y eventos donde se utilizaron cámaras de grabación de video y vigilancia electrónica.

12. **26 de abril de 2018** – Se envía el cuarto "Habeas Data". Surge a consecuencia de que el Hon. Denis Márquez Lebrón notificó información adicional a la CDC en la que indicó que participó de una manifestación donde presenció a personas que parecían de una compañía de seguridad privada grabando a los manifestantes. Se solicitó información a la Policía sobre su rol en dichas actividades, si subcontratan compañías privadas para las grabaciones de eventos públicos, entre otros asuntos relacionados.
13. **4 de mayo de 2018** – La Comisión envió un "Habeas Data" a Liberty Cablevision of Puerto Rico y le requirió información sobre las prácticas habituales de ISPs en Puerto Rico en cuanto al recibo de solicitudes de información personal por agencias de orden público.
14. **31 de mayo de 2018** Reunión en las oficinas de Liberty Cablevision of Puerto Rico para discutir los asuntos atendidos en el requerimiento de información del 4 de mayo de 2018.
15. **6 de junio de 2018** – Quinto Requerimiento de Información "Habeas Data", sobre la utilización de drones por parte de la Policía, las especificaciones de la herramienta, cuál es el proceso para obtener los permisos por parte de la PPR para su uso, el estatus de los permisos, y si se solicita cooperación de locales cercanos a la manifestación para que graben manifestantes, entre otros.

16. **1 de noviembre de 2018** – Reunión con el Dr. Juan Carlos Rivera Hernández, Director del Negociado de Tecnología Informática de la Policía de Puerto Rico, para discutir las funciones de su oficina y su rol en la identificación de nueva tecnología para adquisición, entre otros asuntos.

IV. Información recopilada

Tanto los requerimientos de información como las vistas públicas y reuniones ejecutivas realizadas permitieron a esta Comisión recopilar y analizar información en torno a las siguientes cuatro áreas generales de investigación:

1. Prácticas de monitoreo por parte de agentes de orden público en redes sociales.
2. Prácticas de recopilación de información privada digital durante el ejercicio de funciones investigativas.
3. La grabación de actividades de protesta pública con cámaras de video y audio.
4. El uso de otra tecnología de información en la Policía de Puerto Rico para fines investigativos.

A continuación se presentan los hallazgos principales en estas cuatro áreas, en el orden descrito.

A. Prácticas de monitoreo por parte de agentes de orden público en redes sociales.

En primer término, es importante establecer el contexto en que se suscitan los hechos que dan base a este informe. Ante la situación económica de Puerto Rico, y las medidas de austeridad fiscal que ello ha implicado para el país y para el ofrecimiento

de servicios esenciales,[16] la sociedad civil se ha visto precisada a recurrir a su derecho a la protesta. Las manifestaciones públicas en el país han sido eventos recurrentes durante los pasados años, particularmente en la fecha del 1ro de mayo, cuando se celebran actos políticos en ocasión del Día Internacional de los Trabajadores y Trabajadoras. Los eventos a los que se contrae este informe están relacionados con las actividades del 1ro de mayo de 2017. Según descrito por la Dra. Vicente:

> El día 1ro de mayo de 2017 miles de personas se lanzaron a las calles de Puerto Rico a protestar por las medidas de austeridad adoptadas o programadas por el gobierno y la Junta de Control Fiscal. La concurrida manifestación rechazaba el anunciado recorte millonario al presupuesto de la Universidad de Puerto Rico. Sindicatos, organizaciones feministas, proyectos de defensa de los derechos humanos, grupos religiosos, líderes políticos y miles de compatriotas se unieron para reclamar la auditoría de la deuda, la restructuración de la deuda pública, respeto a la autonomía universitaria y la priorización del presupuesto gubernamental para la atención de las necesidades esenciales del pueblo.[17]

Durante las actividades de protesta de mayo de 2017 ocurrieron unos pocos incidentes de carácter violento, incluyendo daño a la propiedad y enfrentamientos entre la Policía de Puerto Rico y algunos manifestantes, quienes fueron arrestados. El manejo por parte de la Policía de Puerto Rico de estos eventos ha sido criticado por el Asesor Técnico quien está a cargo de verificar el cumplimiento de la Policía con un acuerdo de reforma institucional establecido entre el Departamento de Justicia de Estados Unidos y el Gobierno de Puerto Rico como parte de un litigio ante la Corte de Distrito

---

[16] Véase Hiram Meléndez Juarbe, *In the Red: Puerto Rico's Fiscal and Democratic Deficits Laid Bare* (Quaderni Costituzionali 2017 No. 3), disponible en https://ssrn.com/abstract=3022151

[17] Esther Vicente, La Criminalización de la Protesta en Tiempos de Crisis, Ponencia presentada en el Seminario sobre Teoría Política y Constitucional en América Latina (SELA), el 8 de junio de 2018, publicación en proceso por SELA 2018.

Federal para el Distrito de Puerto Rico, por violaciones de derechos constitucionales por la Policia de Puerto Rico.[18]

Conforme hemos reseñado anteriormente, unos días antes del primero de mayo (el 26 de abril de 2017), la entonces Superintendente de la Policía, Michelle Hernández de Fraley, emitió ciertas expresiones sobre el monitoreo en redes sociales por ese cuerpo. Las mismas denotaron, *prima facie*, prácticas institucionales dirigidas a supervisar y vigilar la conducta de las personas involucradas en actividades de protesta pública. Así, por ejemplo, destacamos expresiones a los efectos de que "[e]stamos monitoreando las redes sociales tenemos acceso a lo que se ha manifestado de las diferentes organizaciones" y que "todo el mundo postea [en Facebook] sus intenciones y nosotros monitoreamos esas intenciones y corroboramos que las intenciones son más que palabras".

En la Audiencia Pública del 5 de julio de 2017, la entonces Superitendente tuvo la oportunidad de elaborar en torno al alcance de estas expresiones. Por su importancia, transcribimos parte de esta explicación de la Superintendente:

> La realidad de estas nuevas plataformas de difusión de información es que carecen de expectativas razonables de intimidad, dado a que se comparten entre usuarios que, a su vez, comparten esa información con otras personas.
>
> Hace poco más de dos meses realicé unas expresiones públicas **que fueron motivadas por los actos de vandalismo que todo el país pudo observar y que se cometieron después que miles de personas acudieron a manifestarse en el área de Hato Rey**. Es meritorio establecer que la Policía de Puerto Rico brindó el más absoluto apoyo a

[18] Para una evaluación de estos eventos, véase *Assessment Report, Police of Puerto Rico's Response to the demonstrations and incidents involving the Capitol building, the "Centro para Puerto Rico" and the Worker's Day*, Office of the Technical Compliance Advisor to the Agreement for the Sustainable Reform of the Puerto Rico Police Department, Case 3:12-cv-02039, Document 712-1, Filed 01/26/18.

los manifestantes, garantizando que pudieran ejercer su derecho a expresarse libremente, protegiendo sus vidas cuando transitaron por las avenidas más concurridas del país. Manteniendo control y orden para que los ciudadanos que estaban allí, expresando sus ideas pudieran hacerlo de forma segura. Este fue nuestro compromiso en la pasada manifestación y seguirá siendo nuestro compromiso en futuras manifestaciones multitudinarias, la seguridad de los manifestantes.

....

La Policía de Puerto Rico, en respuesta a los mensajes y confidencias recibidas por ciudadanos sobre ataques, agresiones y amenazas días antes de la manifestación, dije que estamos monitoreando las redes sociales. Mis expresiones responden a la confirmación de la realización de dicha práctica dentro de un total ambiente de legitimidad, respetando las libertades individuales, pero recibiendo el insumo de la información que se publica en las plataformas digitales y medios noticiosos del país. La misma información que está disponible para cualquier persona que accede a las redes sociales también está disponible para la Policía. ...

La Policía de Puerto Rico garantiza que no está llevando a cabo búsquedas particulares de personas por el mero hecho de expresarse contra el gobierno o sus entidades. No estamos para eso, no es nuestro objetivo. Y tenemos como norte el cumplimiento de los mandatos constitucionales que juramos defender.

Ahora bien, la información que está pública lo está para todos. Observar y recibir información mediante las redes sociales es uno de los mecanismos que utiliza la policía para prevenir efectivamente que se cometan delitos. De igual manera, recibimos confidencias mediante nuestras líneas telefónicas anónimas. Tenemos informantes o cooperadores en la calle, personas que se acercan a nosotros para pedir ayuda y muchas otras maneras disponibles para que podamos ser efectivos.[19]

De lo anterior se desprende que la postura de la Policía de Puerto Rico ante la Comisión fue que esta agencia no monitorea afirmativamente a personas por razón de sus expresiones sino que, en cambio, el monitoreo realizado en anticipo al primero de

[19] Transcripción Audiencia Pública, 5 de julio de 2017, págs. 7-10.

mayo de 2017 fue más bien reactivo—en respuesta a "mensajes y confidencias recibidas por ciudadanos sobre ataques, agresiones y amenazas días antes de la manifestación". Asimismo, indicó que esta información se adquiere de elementos que están en redes sociales a plena vista, disponibles a otras personas.

En respuesta al requerimiento de información del 30 de mayo de 2017, la Policía de Puerto Rico declaró que "no ha creado expedientes de personas y/o entidades como resultado de investigaciones en redes sociales"[20]. Además, indicó que es la División de Crímenes Cibernéticos la que monitorea personas a través de las redes sociales bajo el protocolo establecido en la Orden General Núm. 600-613, titulada "Normas para Solicitar, Monitorear, Intervenir y Procesar las Actividades Relacionadas a Crímenes Cibernéticos", del 29 de agosto de 2014[21]. Esta Orden General estuvo vigente durante todo el periodo bajo investigación hasta que fue enmendada mientras esta investigación estaba en curso (el 25 de abril de 2018). La misma contiene las normas aplicables a los casos en los que se lleva a cabo una investigación en las redes sociales, y establece cómo se almacena información obtenida a través de las redes sociales, dónde se almacena y cómo se dispone de ésta, entre otras cosas, según se discutirá más adelante

[20] Contestación a Tercera Citación y Requerimiento de Información "Habeas Data" a la Superintendente de la Policía de Puerto Rico, Coronela Michelle Hernández de Fraley, con fecha de 30 de mayo de 2017, y contestado el 7 de junio de 2017, donde se solicitó información y documentos relacionados a las alegaciones de monitoreo de redes sociales y a la grabación de eventos públicos, inciso 1.

[21] La Orden General 600-613 de 2014 fue derogada por la Orden General 600-613 de 25 de abril de 2018, ahora titulada "División de Crímenes Cibernéticos". Esta tiene el propósito de establecer la estructura organizacional y funcional de la División de Crímenes Cibernéticos ("DCC"), además de establecer los deberes, normas y procedimientos a seguir por todos los Miembros del Negociado de la Policía de Puerto Rico (en adelante "MNPPR) adscritos a ésta y detallar los servicios de apoyo y las herramientas tecnológicas para que todo MNPPR pueda identificar y realizar una búsqueda de información que permita identificar al sospechoso y agilizar las investigaciones criminales en curso. Se establecen además, las normas y procedimientos para solicitar, intervenir y procesar las actividades y equipos electrónicos relacionados con la comisión de delitos.

En la mencionada Orden 600-613, vigente para la fecha en que se suscitaron las expresiones de la Superintendente, se establecía en su sección IV que:

> La División de Crímenes Cibernéticos **realizará monitoreos de las redes sociales**, Forums, Blogs, IRC Chats, App Messenger, páginas de anuncios clasificados, entre otros. **Cuando se detecte actividad sospechosa relacionada a pornografía infantil, trata humana o cualquier otra actividad delictiva, o de recibirse la información directamente de un ciudadano o por cualquier otro medio, se tomarán las siguientes medidas de acción**: [la Orden General detalla ciertos pasos que deben tomarse en estos casos para captar una imagen de la conducta en cuestión, así como su catalogación y archivo, entre otras cosas que se discutirán oportunamente].

Como se desprende de este texto, la Orden General entonces vigente específicamente establecía la autoridad de la División de Crímenes Cibernéticos de la Policía para "**realizar monitoreos de las redes sociales**" como una actividad fundamentalmente desregulada. Solamente luego de encontrarse actividad sospechosa en ciertos casos, actividad delictiva o tras recibirse la información por una fuente, sólo en esos casos, es que se activarían ciertos requisitos procesales. La ausencia de criterios para controlar esta discreción es patente. En una aparente contradicción, sin embargo a preguntas de la Comisión durante la Audiencia Pública del 5 de julio de 2017, tanto la Superintendente de la Policía como el Sargento Luis Maldonado, director de la División de Crímenes Cibernéticos, testificaron que la Policía no realiza monitoreo *motu proprio* sino que ello se produce en respuesta a confidencias e información recibida a través de un "Fan Page" de Facebook de la Policía. Según expresó el Sargento Maldonado— "en términos de monitorear, no es que nosotros estamos con un 'search engine' buscando,

sino que tenemos este 'Fan Page' en la cual personas ahí... que saben que existe, pues ahí nos refieren amenazas."[22]

En varios momentos, la Policía recalcó su insistencia de que no existe monitoreo proactivo, sino que dependen de información recibida a través del Fan Page de Facebook para dirigir su atención a actividad en redes sociales, y otras fuentes incluyendo transmisiones en vivo en redes sociales de medios noticiosos.[23] En la audiencia pública del 5 de julio de 2017, se interrogó específicamente sobre si existía alguna directriz para que el monitoreo en redes sociales por parte de agentes adscritos a la División de Crímenes Cibernéticos sea sólo en *reacción* a información recibida en el Fan Page (u otras fuentes) y no, por ejemplo, mediante búsqueda proactiva de personas u organizaciones vinculadas a un evento multitudinario como la protesta del 1 de mayo de 2017. La Superitendente nos indicó que "no es la misión de [los agentes adscritos a la División] estar haciendo eso", refiriéndose a la búsqueda proactiva, ya que "ese no es el comportamiento dentro de esta sección, la cual ha sido certificad[a] para hacer este trabajo."[24] Durante la Inspección Ocular del 16 de febrero de 2018 a las facilidades de la División de Crímenes Cibernéticos, el Director de esta División (el Sargento Luis Maldonado), indicó que esa División no utiliza programas de computadora para monitorear movimientos en redes sociales, no monitorean las redes sociales y no ha recibido instrucción alguna para monitorear redes.

[22] Transcripción Audiencia Pública, 5 de julio de 2017, págs. 17-18.
[23] Id. Págs. 20, 50, 67.
[24] Id. Pág. 27.

No obstante lo anterior, la Policía de Puerto Rico testificó que para los eventos del 1 de mayo de 2017, no se crearon expedientes relacionados con querellas presentadas o información recibida sobre expresiones en redes sociales. Es decir, aunque se indicó que los monitoreos en cuestión previo a las manifestaciones del 1ro de mayo de 2017 **fueron motivados por mensajes y confidencias en redes sociales aparentemente conectadas con potenciales actos violentos**, se indicó a la Comisión que en la Policía no había registro de estas confidencias. En cambio, la Policía sí proveyó información a esta Comisión de seis referidos realizados al Federal Bureau of Investigation (FBI) por expresiones en Facebook entre el 28 de abril y el 1 de mayo de 2017, luego de recibir confidencias en torno a alegadas amenazas a la seguridad pública. Tampoco se produjo evidencia del registro de las confidencias que dieron lugar a los referidos al FBI. **Nótese que estas expresiones referidas al FBI fueron realizadas con fecha posterior a los artículos noticiosos (del 26 de abril de 2017) en que se reportaron los comentarios de la Superintendente sobre el monitoreo de la Policía.**

En cuanto al momento en que llegó la información a la Policía, el Sargento Maldonado expresó: "En ese caso del 29 al 1 de mayo la información **que nos llegó**, que representa amenaza a la seguridad pública, como era uno de ellos que dijo que iba a quemar el Capitolio, pues lo trabajó el FBI…".[25] Notamos, sin embargo, una de las expresiones que fue objeto de una acusación federal y que aparece reportada al FBI el 29 de abril de 2017, aparentemente ocurrió el 28 de abril según la declaración jurada

[25] Transcripción Audiencia Pública, 5 de julio de 2017, pág. 59.

del agente federal que sirvió de apoyo a la acusación. En todo caso, debido al momento en que se realizaron, se trata de manifestaciones en Facebook que nada tienen que ver con las expresiones de la Superintendente del 26 de abril de 2017.

Más allá de esos referidos al FBI, no se abrió un expediente de incidentes potencialmente criminales en redes sociales que, se nos dice, motivaron el monitoreo digital por la Policía. La justificación provista para la ausencia de estos expedientes sobre la conducta monitoreada a través de las redes sociales fue la siguiente: "No levantamos expediente porque no hay señalamiento estatal, que podamos cubrir a nivel estatal."[26] Es decir, la Policía alega que registra estos incidentes "[c]uando hay elementos para un delito contemplable en leyes estatales",[27] como sería el "Código Penal o cualquier ley especial aquí en Puerto Rico".[28] Si no hay violación al ordenamiento jurídico de Puerto Rico, alega que esa información "se descarta" porque, como informó el Sargento Maldonado, "si aquí no tenemos herramientas para trabajar un caso por la vía criminal, no podemos preservar esa información."[29]

Al mismo tiempo, la Policía alega que para los casos que fueron referidos al FBI tampoco se levantaron expedientes en la Policía de Puerto Rico porque se trató de conducta que no constituía un delito al amparo del derecho de Puerto Rico, aunque sí podría constituir delito al amparo las leyes Estados Unidos. Sobre el archivo por la

[26] Transcripción Audiencia Pública, 5 de julio de 2017, pág. 60.
[27] Id. Pág. 62.
[28] Id. Pág. 63.
[29] Id. Pág. 63.

Policía de estos casos referidos al FBI el Sargento Maldonado testificó ante la Comisión:

> [N]o hay una legislación [estatal] que cubra cuando una persona hace expresiones amenazantes, no específicamente a alguien, a un individuo, sino abierto. Por ejemplo, … en una ocasión trabajamos un caso, una persona decía algo "voy a ir a atropellar a los vagabundos". Pues ese tipo de caso no está amenazando a alguien en particular. Pero nos preocupa la situación…. [C]uando vemos que ese tipo de expresión se hace, pues le pasamos la información a la agencia federal que sí hay amplia legislación federal con relación a las amenazas cuando se hacen utilizando el "internet".[30]

Los comentarios en Facebook reportados a la Policía, según esta alegó, y que a su vez refirió al FBI fueron todos catalogados como "amenaza", y sobre ellos la Policía de Puerto Rico preservó los referidos al FBI, pero no los comentarios o confidencias recibidas. Una vez referidos estos casos al FBI, terminaba el contacto de la Policía con ellos: "Nosotros la pasamos al FBI por 'e-mail' y no tenemos información… acceso a más información", indicó el Sargento Maldonado en Audiencia Pública.[31]

Se incluyen estos mensajes textualmente, según reflejados en los referidos al FBI:

1. "Vamos a bombardear el Capitolio y que en paz descansen nuestras conciencias" 29 de abril de 2017 (información mediante confidencia sobre persona que emitió esta expresión a través de una cuenta de Facebook).

2. "Ya te queda poco para que te mueras", 29 de abril de 2017 (información mediante confidencia sobre una persona que emitió esta expresión a través de una cuenta de Facebook mientras el Gobernador se encontraba ofreciendo una conferencia de prensa que estaba siendo transmitida desde Facebook).

---

[30] Transcripción Audiencia Pública, 5 de julio de 2017, pág. 60.
[31] Id. Pág. 61.

3. "Que prendan en fuego el capitolio", 29 de abril de 2017 (información mediante confidencia sobre una persona que emitió esta expresión a través de una cuenta de Facebook)

4. "Los que están haciendo la huelga que se pasan en el medio de la calle parando el tránsito"; "En volanta se van tos"; "No llega el día que un Kbrn de una huelga se pare al frente de la guagua y no me deje pasar…."; "fácil y sencillo usted se dirige donde un policía y le pregunta que si puede sacarlos del medio la respuesta del oficial que no y su acción será darle para alante a su vehículo y atropellarlo por lo que están reteniendo en contra de su voluntad y usted teme por su vida"; "únete conmigo este primero de mayo para que los atropellados sean más y los tapones menos", 30 de abril de 2017 (información mediante confidencia sobre persona que emitió esta expresión a través de una cuenta de Facebook)

5. "Si va a estar Ricardo Rosello voy a darle 40 tiros", 1 de mayo de 2017 (información mediante confidencia sobre persona que emitió esta expresión a través de una cuenta de Facebook)

6. "Eso es, que hagan lo que tengan que hacer, que exploten el capitolio si es necesario. Una revolución es lo que hace falta. Me llena de alegría ver la gente molesta, bloqueen todo puñeta. Maten a los policías hagan historia puñeta. Tiren lo que haya que tirar, exploten lo que tengan que explotar, una revolución es lo que hace falta", 1 de mayo de 2017, (información mediante confidencia sobre persona que emitió esta expresión a través de una cuenta de Facebook)

Muchos de estos comentarios en Facebook se perciben, al menos de su faz, como expresiones constitucionalmente protegidas por el derecho a la libertad de expresión según se discutirá en este informe.

Es importante destacar que al menos una de las personas referidas por la Policía de Puerto Rico al FBI por comentarios en Facebook, fue inmediatamente arrestada y acusada por las agencias federales de ley y orden por alegada violación a un delito federal de amenazas tipificado en 18 USC § 844(e), el cual acarrea una pena de hasta

10 años de cárcel.[32] La acusación federal fue presentada el 29 de abril de 2017, tan pronto como la Policía refirió el asunto al FBI por la persona expresar "Vamos a bombardear el Capitolio y que en paz descansen nuestras conciencias".[33] Ese mismo día fue arrestada la persona en su lugar de trabajo, según reportado en la prensa escrita.[34] Ese mismo día también, **dos días antes de los eventos del 1ro de mayo**, la fiscal federal para el Distrito de Puerto Rico, Rosa Emilia Rodríguez, comunicó a todos los medios del país el arresto de esta persona, manifestando la fiscal que "[h]ay una línea muy fina entre la libertad de expresión y el incitar a la violencia. Cuando esa línea se cruza, la expresión no es protegida porque se convierte en una conducta criminal."[35] Todos los medios principales del país reseñaron este arresto, el cual también fue ampliamente discutido en las redes sociales. Por ejemplo, El Vocero, El Nuevo Día, Primera Hora y Noticel cubrieron la noticia, y al menos un comunicador con más de 1 millón y medio de seguidores en Facebook publicó el asunto.[36] Todo ello, a menos de 48 horas de llevarse a cabo la manifestación convocada para el 1ero de mayo de 2017s protestas.[37]

---

[32] 18 USC 844(e) ("(e) Whoever, through the use of the mail, telephone, telegraph, or other instrument of interstate or foreign commerce, or in or affecting interstate or foreign commerce, willfully makes any threat, or maliciously conveys false information knowing the same to be false, concerning an attempt or alleged attempt being made, or to be made, to kill, injure, or intimidate any individual or unlawfully to damage or destroy any building, vehicle, or other real or personal property by means of fire or an explosive shall be imprisoned for not more than 10 years or fined under this title, or both.")

[33] Acusación federal radicada el 29 de abril de 2017 en la Corte Federal de Distrito para el Distrito de Puerto Rico en contra de Iván Zayd Guillama-Rosario. Número de caso 3:17-mj-857-SCC.

[34] *Arrestan a un hombre por amenazar con bombardear el Capitolio*, El Nuevo Día, 29 de abril de 2017, https://www.elnuevodia.com/noticias/seguridad/nota/arrestanaunhombreporamenazarconbombardearelcapitolio-2316199/.

[35] Comunicado de Prensa del 29 de abril de 2017 "Individual Arrested For Threatening To Bomb El Capitolio", https://www.justice.gov/usao-pr/pr/individual-arrested-threatening-bomb-el-capitolio.

[36] *Arrestan hombre por amenazar vía Facebook de bombardear el Capitolio*, Primera Hora, 29 de abril de 2017, https://www.primerahora.com/noticias/puertorico/nota/arrestanhombreporamenazarviafacebookdebombardearelcapitolio-1220964/; *Federales arrestan hombre que convocó a bombardear el Capitolio*, NotiCel, 29 de abril de 2017, https://www.noticel.com/la-calle/federales-arrestan-a-hombre-que-convoc-a-bombardear-el-capitolio/609160987.

[37] 30 de abril de 2017, Publicación en Facebook Oficial de Molusco, http://www.facebook.com/ElMolus.

Los cargos contra la persona arrestada en su lugar de trabajo e imputada por la comisión de un delito federal fueron desestimados el 23 de agosto de 2018.[38]

Si bien la Superintendente declaró que la Policía de Puerto Rico estuvo "monitoreando las redes sociales" sólo "en respuesta a los mensajes y confidencias recibidas por ciudadanos sobre ataques, agresiones y amenazas días antes de la manifestación", cabe destacar que no brindó a esta Comisión información específica sobre estos "mensajes y confidencias recibidas por ciudadanos" que alegadamente activaron un monitoreo de redes sociales. La razón aparente por la que no se almacenó o registró formalmente esta información por la Policía, según sus declaraciones, fue que esa agencia no retiene información de conducta que **no constituye delito** en Puerto Rico. Ello presenta una interrogante importante: si estas expresiones no constituyen delito en Puerto Rico, ¿por qué se incurrió en el extraordinario monitoreo del que habló la Superintendente en los medios el 26 de abril de 2017, y que luego defendió en Vista Pública?

En fin, aun si tomamos como cierta la palabra de la entonces Superitendente de que en efecto hubo monitoreo de redes sociales durante el periodo previo a las manifestaciones del 1ro de mayo de 2017. Esta Comisión no tiene constancia de las razones que motivaron el monitoreo. Sí hay base para concluir que, cualesquiera hayan sido estas razones, no se trató de denuncias en redes sociales sobre conducta delictiva en esta jurisdicción. De otro lado, esta Comisión puede constatar que la Policía refirió

[38] Orden de Desestimación del Caso Núm. 3:17-mj-857(SCC), 23 de agosto de 2018, por la Jueza Hon. Silvia Carreño-Coll (Docket No. 19).

al FBI ciertas expresiones y comentarios en Facebook entre el 28 de abril y el 1 de mayo (posteriores a las expresiones de la Superintendente en los medios) sobre asuntos que la Policía se entiende sin jurisdicción y, en un caso, las agencias federales realizaron un arresto inmediato y denuncia (eventualmente desestimada), lo cual procuraron anunciar a todo el país justo antes de las manifestaciones políticas.

La Policía de Puerto Rico tampoco proveyó información sobre perfiles, cuentas de redes sociales o páginas de internet de personas u organizaciones que han sido o actualmente están siendo monitoreadas por la PPR, alegando que dicha información no existe en el Negociado.[39] Se indicó, además, que la PPR no intervino, arrestó o citó a persona alguna como resultado de un monitoreo de redes sociales en el contexto de las protestas del 1ro de mayo de 2017.[40] Igualmente, se nos indicó que la PPR no solicitó órdenes judiciales a un tribunal general de justicia producto del mencionado monitoreo.[41] Tampoco se proveyó la lista de perfiles creados por la PPR para realizar su trabajo ya que adujeron su confidencialidad, pues "se trata de investigaciones criminales en curso".[42]

En fin, esta Comisión de Derechos Civiles no pudo constatar cuáles fueron, ni cuál fue la gravedad de las advertencias concretas que justificaron asumir una postura

[39] Contestación al primer requerimiento de información "Habeas Data" con fecha de 30 de mayo de 2017, contestado el 7 de junio de 2017, inciso 11.
[40] Id. Inciso 12.
[41] Id. Inciso 17.
[42] Id. Inciso 8.

de monitoreo en redes sociales sobre personas o grupos, según articuló la Superintendente en los medios de comunicación.

En términos organizativos y operacionales, es oportuno recalcar que las gestiones relacionadas con el monitoreo, intervención y procesamiento de actividades relacionadas a los llamados crímenes cibernéticos están a cargo de la División de Crímenes Cibernéticos, antes mencionada.

La División de Crímenes Cibernéticos de la Policía de Puerto Rico está adscrita a la Superintendencia Auxiliar en Investigaciones Criminal según la Orden General 100-102, "Estructura del Negociado de la Policía de Puerto Rico, del 13 de noviembre de 2018 y de conformidad con la Orden General 100-107, "Reorganización de la Superintendencia Auxiliar en Investigaciones Criminales", de 30 de junio de 2017. Durante todos los eventos pertinentes, los parámetros de acción de la División de Crímenes Cibernéticos estuvieron, a su vez, regidos por la Orden General 600-613. "Normas para Solicitar, Monitorear, Intervenir y Procesar las Actividades Relacionadas a Crímenes Cibernéticos", del 29 de agosto de 2014. Durante el transcurso de esta investigación, como ya hemos señalado, el 28 de abril de 2018, se aprobó una nueva Orden General 600-613, titulada "División de Crímenes Cibernéticos", para reglamentar las operaciones de dicha división.

La División de Crímenes Cibernéticos era dirigida al momento de realizarse la investigación de la querella por el Sargento Luis Maldonado Miranda y contaba con dos (2) servidores; ocho (8) computadoras tipo "laptops"; quince (15) computadoras

tipo "desktops"; y once (11) empleados bajo la dirección del Sgto. Maldonado.[43] Según información brindada en la Vista Pública celebrada el 5 de julio de 2017, esta División atiende entre 1,200 y 1,400 casos anuales, de los cuales aproximadamente 400 tienen que ver con conducta en las redes sociales. La mayor parte de los asuntos atendidos se relacionan con situaciones de amenazas, violencia doméstica, acoso y asuntos similares.[44]

La Orden General 600-613 del 20 de agosto de 2014 (vigente a la fecha de los eventos pertinentes a la querella investigada) estableció que la División de Crímenes Cibernéticos fue creada para (a) "brindar apoyo técnico especializado a la rama investigativa tanto de las Áreas Policiacas como a nivel central"; (b) realizar "las investigaciones donde requiera personal técnico especializado en el uso de equipo computadorizado"; así como (c) "detectar y esclarecer la actividad criminal mediante el uso de informática que incluye fraude electrónico, pornografía infantil, falsificación y acceso no autorizado".[45]

Entre los servicios de apoyo técnico que la División ofrece a la Policía, según esta orden, se encuentran:

1. Ofrecer asistencia en la investigación de cualquier otro delito tradicional en donde en alguna parte de la investigación se descubre que el sospechoso utilizó algún medio en Internet.

2. Brindar apoyo en solicitudes de evidencia reservada en los historiales de los sistemas informáticos a las diferentes compañías y recursos en Internet.

---

[43] Contestación al tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 34.

[44] Expresión del Sargento Maldonado en Audiencia Pública de 5 de julio de 2017, pág. 65, líneas 3-16 de su transcripción.

[45] Orden General 600-613 de 29 de agosto de 2014, "Normas para Solicitar, Monitorear, Intervenir y Procesar las Actividades Relacionadas a Crímenes Cibernéticos", Parte I, Propósito.

3. Analizar mensajes de correo electrónico implicados en la comisión de delitos, se analizan direcciones web (URL) dominios, "websites" o cualquier medio de emisión y difusión de información en Internet como "blogs", "fórums", "webcast", "podcast" (RSS), redes sociales, entre otros.

4. Realizar rastreos de direcciones de protocolo de Internet (IP Address).[46]

En términos del Monitoreo en las redes sociales, como se explicó anteriormente, la Orden General 600-613 del 20 de agosto de 2014, establecía en su Parte IV que la División "**realizará monitoreos de las redes sociales**", así como en otros espacios digitales. Ahora bien, cuando "se detecte **actividad sospechosa relacionada a** pornografía infantil, trata humana o **cualquier otra actividad delictiva**, o de **recibirse información directamente de un ciudadano o por cualquier otro medio** se tomarán las siguientes **medidas de acción**":

a. El Agente Investigador Cibernética asegurará la información mostrada en la página web realizando una captura de pantalla marcando las teclas (Ctrl+PrtScn) en el teclado y luego importar dicha captura en un documento formato Word (doc). Puede además, utilizar la herramienta "snipping tool" en la cual se realiza una captura de la imagen completa que cubra la dirección web (URL) que mostraba el navegador al momento de identificar el contenido; asegurar que se vea fecha y hora si es una conversación o mensaje. luego guardar en formato Jpeg ó Pdf y e incluir el hash para cada file ya sea foto, audio, video, una conversación, una imagen, un Log de sesión o algún código html.

b. Asignará un número de control y crear un archivo digital con la información. Colocar en la carpeta bajo casos sin querella y notificará a la División de Delitos Sexuales y/o a HSI, ICE, FBI.

---

[46] Orden General 600-613 de 29 de agosto de 2014, "Normas para Solicitar, Monitorear, Intervenir y Procesar las Actividades Relacionadas a Crímenes Cibernéticos", Parte II, Funciones y Responsabilidades de la División de Crímenes Cibernéticos.

c. Verificará el tipo de información que colecta la compañía. Para ello ir a los "Privacy Policy" de la página web.

....

f. Si un Agente Investigador Cibernético identifica a través de un medio de información telemática una actividad delictiva, se le notificará a la unidad investigativa que corresponda para que el Director de la Unidad Especializada asigne a un Agente para trabajar en conjunto la investigación y el curso general del caso.

g. El agente Investigador asignado será responsable de asignar un número de querella al caso.

....

[j.] Una vez el Agente investigador de Distrito Precinto o Unidad Especializada, sea notificado, será responsable de recoger los documentos del caso. En los casos que se determine que haya un delito grave, éste consultará con Fiscalía local para las denuncias correspondientes. En los casos de delitos menos grave, el Agente investigador de Distrito, Precinto o Unidad Especializada, será responsable de continuar la investigación para su radicación en los Tribunales.

De lo anterior se desprende que, una vez se detecta "**actividad delictiva**" en internet, o se recibe información "**directamente de un ciudadano o por cualquier otro medio**", se activa un protocolo de acción que incluye: (a) tomar imágenes en computadora de la conducta en cuestión; (b) asignar un número de control y crear un archivo digital con la información; y (c) referir la información a los componentes investigativos y del Ministerio Público pertinentes, entre otras cosas. Este protocolo de acción fue reiterado a esta Comisión en sus elementos esenciales durante la Inspección Ocular a las facilidades de la División realizada el 16 de febrero de 2018. Resulta pertinente, además, que la referida Orden General además contenía una serie de "Controles Administrativos" que exigían el registro y documentación de toda

solicitud de servicio por un agente o ciudadano, entre otras medidas. Como se ha dicho, las alegadas expresiones en redes sociales que, se nos informa, fueron recibidas por el Fan Page de Facebook de la Policía no fueron objeto de estas "medidas de acción".

Cabe destacar que la nueva Orden General 600-613 del 25 de abril de 2018, aprobada durante el transcurso de esta investigación, y que reemplaza la Orden vigente durante las protestas del 1ro de mayo de 2017, mantiene un lenguaje similar al antes descrito, pero reemplaza la norma de que la División "realizará monitoreos" con la frase "evaluará toda información recibida", en un aparente esfuerzo por rectificar la postura sobre el monitoreo proactivo recogida en el texto de la Orden anterior, pero negada durante el testimonio ofrecido a esta Comisión.[47] Asimismo, la nueva Orden General establece en su Parte V(B)(1) que "se prohíbe a todo [Miembro del Negociado de la Policía de Puerto Rico] que, sin un fin legítimo, levante, mantenga, preserve, recopile información personal de individuos, organizaciones, agrupaciones, si dichos individuos, organizaciones y agrupaciones no están vinculados con la comisión o intento de cometer un delito."

[47] La nueva Parte P de dicha Orden General se titula "Procedimiento para la Recopilación de Información de Actividades Delictivas Cibernéticas" y contiene el siguiente texto:

> "La DCC **evaluará toda información recibida** sobre actividad delictiva en las redes sociales, foros, blogs, IRC Chats, App Messenger, páginas de anuncios clasificados, entre otros. Cuando, de la información recibida se identifique actividad sospechosa relacionada a pornografía infantil, trata humana o cualquier otra actividad delictiva, ya sea información recibida directamente de una persona o por cualquier otro medio, los agentes investigadores cibernéticos tomarán las siguientes medidas de acción: [detallando un protocolo similar a la Orden General anterior]"

B. Prácticas de recopilación de información privada digital durante el ejercicio de funciones investigativas

La investigación sobre las prácticas de monitoreo electrónico por parte de la Policía de Puerto Rico condujo a esta Comisión a indagar en torno a las políticas y prácticas institucionales relacionadas con la solicitud de información personal digital, que se encuentra en manos de terceros, como es el caso de información sobre usuarios de plataformas de redes sociales, o almacenada por proveedores de servicio de internet, entre otros. Es decir, esta Comisión se planteó dos cuestiones fundamentales: Primero, una vez identificada la potencial conducta delictiva como producto de referidos o monitoreo en las redes sociales, ¿qué pasos se toman para obtener información privada que está almacenada en servidores de los servicios computadorizados utilizados por las personas, y cuál es la información que se obtiene? Segundo: estas prácticas y políticas ¿se ajustan al derecho estatutario y constitucional vigente en esta jurisdicción? En esta sección se describen los hallazgos principales alrededor de la primera de estas preguntas. La legalidad de estas prácticas, se considerará más adelante en este informe.

Como se describió en la sección anterior, una vez un agente investigador de la División de Crímenes Cibernéticos identifica una actividad delictiva, se le asigna un número de control y se crea un archivo digital, de conformidad con la Parte IV de la Orden 600-613 del 29 de agosto de 2014 (vigente al momento de los eventos bajo estudio). En esta misma Parte, la referida Orden establecía algunos elementos relacionados con la obtención de información privada almacenada en servidores de los servicios en internet utilizados por las personas:

d. Una vez se documenta el caso, [el Agente Investigador Cibernético] solicitará una preservación de datos a la compañía de servicios web o red social que ofrece tales servicios. (Stored Communications Act 18 US Code 2701-12).

e. La solicitud de preservación de datos no deberá realizarse a un término de más de noventa (90) días de la ocurrencia de los hechos.

....

h. La División de Crímenes Cibernéticos investigará y asesorará en lo referente a la cibernética. Se pondrá en contacto con el fiscal de la UICC del Departamento de Justicia [(Unidad Investigativa de Crímenes Cibernéticos)] para que asista en el caso y trabajará con la fiscalía local cualquier Subpoenas u Órdenes de Registro (Search Warrants) correspondientes, según aplique.

i. Tramitará el subpoena y/o la orden de registro y recibirá la información por parte de la red social, compañía de recursos Web ISP (proveedora de servicios de Internet), será analizada. Se le notificará al Agente Investigador que sometió la querella una vez se culmine la investigación o se requiera información adicional sobre el caso.

Se desprende de lo anterior que, en términos generales, una vez se detecta conducta potencialmente delictiva, observada en las redes sociales, la División de Crímenes Cibernéticos toma las siguientes acciones: (a) solicita a la plataforma de internet que preserve información relevante, toda vez que podrá ser solicitada como parte de un proceso investigativo; (b) coordina con el Ministerio Público (en particular la Unidad Investigativa de Crímenes Cibernéticos del Departamento de Justicia), la preparación y presentación de *subpoenas* u órdenes judiciales de registro para solicitar información, según aplique y (c) tramita el *subpoena* u orden de registro y recibe la información personal por parte de la plataforma digital, para su evaluación y análisis.

En vista de lo anterior, la Comisión procuró información sobre: (a) el tipo de información personal que se solicita a estos servicios de internet y (b) los mecanismos a través de los cuales se requiere (es decir, en qué circunstancias se requiere información mediando orden judicial o, de otro lado, en qué circunstancias se requiere información mediante *subpoena duces tecum*, que no necesita intervención judicial).

En cuanto a lo primero (el tipo de información solicitada), esta Comisión pudo constatar que en el transcurso de las investigaciones relacionadas con conducta observada en las redes sociales, las agencias de orden público solicitan información como la siguiente a las plataformas de redes sociales (y otras plataformas):

(a) Información del registro de cuenta de las redes sociales (como el nombre, y fecha de creación de cuenta)

(b) Dirección de correo electrónico

(c) Dirección del Protocolo de Internet (Dirección IP) asociado a la computadora con la que se accede al servicio en determinado periodo de tiempo.

(d) Historial de uso de una persona de una red social en determinado periodo de tiempo.

(e) Contenido de las comunicaciones en una red social o plataforma de internet.[48]

Una vez el Estado obtiene la dirección IP asociada a un usuario, provisto por una de las redes sociales o por algún servicio de Internet, de servicios de almancenaje en la nube, de correo electrónico o de comunicación VOIP, puede entonces obtener otra

[48] Información ofrecida por Sargento Maldonado, Director de la División de Crímenes Cibernéticos en Inspección Ocular del 16 de febrero de 2018.

información de otras entidades. Ello implica que puede obtener información de Proveedores de Servicio de Internet, ISP por sus siglas en inglés.

La Dirección IP consiste de un número único asignado, comúnmente por un tiempo definido, a toda computadora conectada a la internet. Este número opera como una dirección a la que llegan, y desde la que se transmiten, paquetes de información digital a otra computadora con otra dirección única de IP.[49] Es usual que esta dirección o número sea asignado a un individuo por el Proveedor de Servicio de Internet (ISP) que utiliza. El ISP asigna a cada usuario una Dirección IP, particular y única, y mantiene récords de esa asignación, una vez la red social provee al Estado la dirección de IP asociada con determinada conducta observada, el Estado puede a su vez recurrir al ISP para que identifique a los clientes a quienes se les asignó un número en particular. En estos casos, la información sobre la clientela de cada ISP que se puede solicitar incluye:

(a) Nombre[50]

(b) Información de contacto[51]

(c) Teléfono[52]

(d) Correo electrónico[53]

(e) Duración del servicio[54]

---

[49] RFC 760, *DOD Standard Internet Protocol*, DARPA, Information Sciences Institute (enero 1980), https://tools.ietf.org/html/rfc760; James Grimmelmann, Internet Law: Cases and Problems 27-39 (2018); Barbara van Schewick, Internet Architecture and Innovation (2010).

[50] Según contestación a Requerimiento de Información "Habeas Data" cursado a Liberty Puerto Rico el 4 de mayo de 2018 y contestado el 14 de mayo de 2018, inciso 2(c).

[51] Id.

[52] Id.

[53] Id.

[54] Orden General 600-613 de 25 de abril de 2018, titulada "División de Crímenes Cibernéticos", pág. 12, inciso III(I)10(d).

(f) Medios o fuente de pago del servicio (incluyendo la cuenta de crédito o cuenta bancaria utilizada)[55]

Al menos un ISP al que esta Comisión tuvo la oportunidad de entrevistar aclaró que en el pasado se le ha solicitado información sobre el historial de visitas de un cliente (como, por ejemplo, qué paginas de internet visitó en determinado momento o en determinado periodo de tiempo). Ello es consistente con lo manifestado por el Director de la División de Crímenes Cibernéticos durante la Inspección Ocular llevada a cabo en las oficinas de la División de Crímenes Cibernéticos. Al mismo tiempo, ese ISP indicó que, aunque se le ha solicitado la información, esta no se almacena en sus sistemas por lo que es incapaz de proveerla.[56]

Notamos, además, que la Orden 600-613 del 29 de agosto de 2014, vigente al momento de los eventos bajo investigación, no contiene una descripción del tipo de información obtenible mediante requerimiento u orden judicial a las plataformas de internet. En cambio, es notable que la versión más reciente de esta Orden, aprobada el 25 de abril de 2018, sí contiene disposiciones que atienden este asunto según se discutirá a continuación.

La segunda cuestión sobre la cual esta Comisión indagó giró en torno al *tipo de procedimiento* utilizado para solicitar información personal que se encuentra alojada en los servidores de las plataformas de internet, ya sea una red social, servicios en la nube, email, buscadores o ISPs, entre otros. Específicamente se trató de aclarar si, por un

[55] Orden General 600-613 de 25 de abril de 2018, titulada "División de Crímenes Cibernéticos", inciso III(I)10(f).
[56] Según contestación a Requerimiento de Información "Habeas Data" cursado a Liberty Puerto Rico el 4 de mayo de 2018 y contestado el 14 de mayo de 2018, inciso 2(d) y (e).

lado, la información se solicita a través de una orden judicial, para la cual un juez debe determinar si existe causa probable, o si, en cambio, se obtiene mediante un requerimiento *no judicial* de información, como lo es el *subpoena duces tecum* que emite una agencia gubernamental de ley y orden sin supervisión de la Rama Judicial. Esta diferencia, aunque procesal, no es trivial. Como ha dicho el Tribunal Supremo de Estados Unidos "la historia de la libertad ha sido en gran medida la historia del cumplimiento con salvaguardas procesales".[57] En el caso del requisito de intervención judicial, se trata de un mecanismo diseñado para proteger "el interés del individuo en la intimidad de su hogar y sus posesiones de una interferencia injustificada por parte del Estado".[58] La intervención judicial, cuando procede, impone "el requisito de que la causa probable esté basada en juramento o afirmación, la exigencia de que la orden incluya una descripción detallada del lugar a ser allanado, las personas y cosas a registrarse y los objetos a ser ocupados".[59] Como se discutirá en una sección subsiguiente, hay circunstancias en que la orden judicial basada en causa probable es un requisito constitucional, y hay otras en que no lo es.

A preguntas de la Comisión, el entonces Director de la Unidad Investigativa de Crímenes Cibernéticos del Departamento de Justicia, Rafael Sosa, articuló las circunstancias en las que el Departamento de Justicia solicita información almacenada digitalmente mediante una orden y mediante un *subpoena*. Por su importancia, se transcribe el testimonio del funcionario:

---

[57] *McNabb v. U.S.*, 318 U.S. 332, 347 (1943) ("The history of liberty has largely been the history of observance of procedural safeguards").
[58] *Pueblo v. Richard Rolón Rodríguez*, 193 D.P.R. 166 (2015), página 11, citando a Olga Elena Resumil, Práctica jurídica de Puerto Rico: Derecho Procesal Penal 277, T.I (1990).
[59] *Pueblo v. Richard Rolón Rodríguez*, 193 D.P.R. 166, 177 (2015).

El estado de derecho actual se rige principalmente por la ley federal, "Electronic Communications Privacy Act", especialmente en esa sección está lo que se conoce como el "Stored Communications Act", en donde establece cuáles son los requisitos para la obtención de evidencia electrónica.

Claro, esto lo establece cuando ya hay una expectativa de privacidad. Así que, cualquier información, como se ha mencionado aquí que es pública, pues ya eso no goza de ninguna expectativa de privacidad, porque así el propio usuario ha escogido compartirlo públicamente.

Cuando la información está protegida, o sea, es privada, esta ley, "Stored Communications Act", establece que **hay información transaccional** y hay **información de contenido**. Información transaccional supone cualquier tipo de información sobra el nombre de la persona, correo electrónico que usó, fecha de registración y otro tipo de información que describe la actividad que está llevando acabo ese usuario, pero no el contenido. Para eso se hace a través de un "subpoena" el requerimiento, directamente al "ISP".

Ahora, ... la misma ley habla sobre los mecanismos, como en muchos casos los agentes deben de preservar la confidencialidad de alguna investigación, para que esa notificación al usuario se demore por un periodo de 90 días.

Ahora, eso no lo puede hacer solamente el agente o solamente por medio de un "subpoena". La ley exige que haya una orden judicial y que se establezca una de cinco razones que están establecidas en el "Stored Communications Act", que justifique que hay una demora en esa notificación. Por ejemplo, el riesgo de que se destruya evidencia, que es un riesgo común en evidencia electrónica.

Así que, para poder hacer lo que se llama en la ley, "Delay Notification", o sea, demorar la notificación por un período de 90 días, la ley establece que un Juez, el Tribunal, tiene que recibir una orden, evaluar unas razones específicas y determinar si se autoriza. Cuando ese Juez autoriza, se le envía al "ISP" ese requerimiento con esas instrucciones, y esa contestación llega al agente.

Si es contenido, entonces se va ya con todos los estándares de una orden de registro y allanamiento, estableciendo causa probable, para poder

> entrar a ese contenido privado. Es la única manera en la cual un agente puede tener acceso a ese tipo de información.[60]

Es decir, el Departamento de Justicia se deja llevar por el régimen establecido por Estados Unidos para solicitar la información que es alojada en los servidores de terceros. Cuando se trata de información catalogada como transaccional, o que no es contenido de comunicaciones, se solicita por medio de *subpoena* (como el "nombre de la persona, correo electrónico que usó, fecha de registro y otro tipo de información que describe la actividad que está llevando acabo el usuario"). En caso de que sea necesario evitar que se le notifique al usuario de una solicitud de información, el funcionario del Departamento de Justicia testificó que el Gobierno puede acudir a un tribunal para solicitar la posposición de la notificación, por hasta un máximo de 90 días, sobre la base ciertas razones que provee el "Stored Communications Act". Ahora bien, cuando se trata del contenido de una comunicación, siempre habrá que solicitarlo mediante una orden judicial.

A preguntas de la Comisión sobre el impacto que puede tener en estos procedimientos la jurisprudencia del Tribunal Supremo de Puerto Rico que establece una protección mayor al derecho a la intimidad, en particular el caso de *Weber v. E.L.A.*[61] (a discutirse oportunamente en este informe), el Fiscal Sosa explicó:

> Nosotros atemperamos a ... *Weber*, los requerimientos.... Fíjese que para efectos de "Stored Communications Act" los registros telefónicos sería información transaccional. Por lo tanto, serían obtenibles por "subpoena".
>
> El hecho de que en Puerto Rico existe una jurisprudencia que reconoce esa privacidad, ... lo que estamos viendo es que el registro de llamadas

[60] Transcripción de Audiencia Pública de 5 de julio de 2017, págs. 31-33.
[61] *Weber Carrillo v. ELA*, et al., 190 D.P.R. 688 (2014).

> **puede revelar patrones o estilos de vida**. Por eso es que entonces el Tribunal Supremo [de Puerto Rico] reconoce que eso se debe pedir por orden de registro y allanamiento, y así nosotros también lo hacemos.
>
> Porque a pesar de que el "Stored Communications Act" le permite al Estado hacer unas búsquedas, eso tiene que ser también conforme al estado de derecho local. Y por ende, un agente aquí en Puerto Rico para poder solicitar un registro de llamadas telefónicas tiene que hacerlo por orden de registro, para atemperarlo a *Weber*, a pesar de que si fuera estrictamente por "Stored Communications" no tuviese que ser así. Pero en Puerto Rico así se pide, por orden.[62]

Es decir, si bien se informó que se siguen los parámetros de la ley federal, a preguntas de la Comisión se aclaró que—al menos en lo que tiene que ver con la información que, como el registro de llamadas de una persona—puede revelar "patrones o estilos de vida"—aunque se clasifique como "transaccional" al amparo de las normas jurídicas de Estados Unidos, se solicita mediante una orden judicial según requiere el más exigente derecho puertorriqueño.

Dicho lo anterior, no quedó del todo claro cuál es el tipo de información que el Departamento de Justicia solicita mediante una orden judicial, más allá de referirse a información de "contenido" y aquella que sería "transaccional" pero que revela "patrones o estilos de vida", según la jurisprudencia de Puerto Rico. Esta Comisión solicitó al funcionario del Departamento de Justicia en audiencia pública la guía interna del Departamento que articule estos criterios de forma precisa. A pesar de que se informó que existían unas "guías de evidencia digital que se circulan a los fiscales"[63] para ayudarles en estos procesos, e inicialmente se indicó durante la Audiencia Pública que se someterían las mismas a esta Comisión, el Departamento de Justicia

[62] Transcripción Audiencia Pública de 5 de julio de 2017, págs. 33-34.
[63] Id. Pág. 39.

eventualmente se negó a brindar estas guías, a pesar de haberse cursardo reiterados requerimientos.[64]

La única fuente de información que arroja luz sobre estos elementos se encuentra en la nueva Orden General 600-613 de la Policía de Puerto Rico, aprobada el 25 de abril de 2018, mientras esta investigación estaba en curso. Dicha Orden contiene una nueva Parte I, que establece la Sección de Requerimientos Legales (o "Legal Requests") adscrita a la División de Crímenes Cibernéticos. Allí se disponen los siguientes parámetros:

> 6. **Toda información basada en contenido**, entiéndase mensajes privados, imágenes, información de ubicación, que se desee obtener de cualquier compañía de servicios de comunicación electrónica como parte de un proceso de investigación de delito, será solicitada a través de una orden de registro o "search warrant". En la misma. se debe establecer una relación o nexo causal entre el delito investigado y la información solicitada, estableciendo así una causa probable que deberá aparecer en la Orden. Para ello, el agente investigador del caso consultará el caso con un fiscal o procurador enlace de la Unidad Investigativa de Crímenes Cibernéticos (en adelante "UICC") del Departamento de Justicia.
>
> ....
>
> 9. **Toda solicitud de información básica de registro**, no basada en contenido, será solicitada a través de un *subpoena*. Para ello, el agente investigador primero consultará el caso con un agente de la Sección de Legal Request de la DCC, quien le proveerá la orientación adecuada y la información de contacto del fiscal o procurador enlace de la UICC del Departamento de Justicia. El agente cibernético de la Sección de Legal Request preparará el

[64] Solicitud cursada al Fiscal Rafael Sosa el 5 de julio de 2017, la cual fue contestada el 7 de julio de 2017, indicando que las guías solicitadas "son una herramienta de trabajo para fiscales y procuradores de asuntos de menores y que debido a la información sensitiva que contienen las mismas, éstas no pueden ser divulgadas". El 5 de diciembre de 2017 se cursó carta a la Secretaria de Justicia, Hon. Wanda Vázquez Garced, haciendo la misma solicitud. En su contestación, recibida el 8 de enero de 2018, el Departamento se sostuvo en la determinación inicial de no divulgar la ifnormación.

subpoena siguiendo las recomendaciones del fiscal o procurador enlace de la UICC del Departamento de Justicia.

10. Con un *subpoena* del fiscal, el proveedor de servicios de comunicación electrónica o de servicios informáticos remotos revelará a la entidad gubernamental solicitante lo siguiente:
    a. Nombre.
    b. Dirección.
    c. Registros de conexión telefónica y duración de llamada para un número telefónico específico.
    d. Duración del servicio (incluida la fecha de inicio) y tipos de servicios utilizados.
    e. Número de teléfono o de instrumento, u otro número o identidad de abonado, incluyendo cualquier dirección de red temporalmente asignada (dirección de IP, o dirección de correo electrónico).
    f. Medios y/o fuente de pago para dicho servicio (incluyendo cualquier tarjeta de crédito o número de cuenta bancaria) de un abonado o cliente de tal servicio.
    g. La ley federal establece que aunque la entidad gubernamental que recibe la información solicitada mediante *subpoena*, no está obligada a proporcionar aviso a un suscriptor o cliente. Dicho esto, internamente las compañías proveedoras de comunicación electrónica podrían notificar a su cliente sobre la petición de información de registro. En circunstancias exigentes, donde el agente investigador entienda que el sospechoso podría destruir evidencia si entra en conocimiento de la solicitud de información, solicitará la información mediante orden del Tribunal y notificará al agente de la Sección de Legal Request de DCC para que solicite una preservación de datos a la compañía proveedora de comunicación electrónica.

Como se observa, la Nueva Orden General reproduce la dicotomía entre información de contenido (que se solicita mediante orden judicial) e información transaccional (la llamada "información básica de registro"), que se solicita por *subpoena* sin notificación a la persona, en aparente fidelidad a la ley federal (Stored Communications Act). En la nueva Orden General no hay mención del procedimiento que se sigue para obtener información que refleja patrones de conductas y estilos de

vida de las personas y que (según el Fiscal Sosa testificó durante la Audiencia Pública) debe solicitarse mediante una orden judicial por virtud de la jurisprudencia del Tribunal Supremo de Puerto Rico. Tampoco se aclara si la información sobre el historial de un usuario (como un registro de páginas o URLs visitadas), debe tratarse como "contenido" o como "información básica de registro".

Finalmente, destacamos que esta Comisión preguntó específicamente a la Policía de Puerto Rico mediante el requerimiento de información del 9 de abril de 2018 si, con relación a los eventos del 1ro de mayo de 2017, solicitó a algún ISP o a cualquier plataforma de redes sociales información sobre el uso de internet o esa plataforma de alguna persona, sea mediante *subpoena* o mediante orden judicial.[65] La contestación de la Policía de Puerto Rico fue: "Ninguna".[66]

C. *La grabación de actividades de protesta pública con cámaras de video y audio*

Por su relación con los hechos que motivaron esta Investigación, la Comisión de Derechos Civiles consideró no solo los elementos relacionados con el monitoreo en las redes sociales, sino también las prácticas y políticas relativas a la grabación mediante cámaras de video y audio por la Policía de Puerto Rico.

En términos organizativos, la división que está a cargo de grabar eventos públicos, así como de archivar el video grabado y mantener el equipo para ello es la *Sección Técnica de Grabaciones*. La ubicación institucional de esta Unidad ha variado

[65] Tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 32.
[66] Contestación al tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 32.

en los últimos años conforme surge de las órdenes generales provistas a la Comisión por la Policía de Puerto Rico.

Para los eventos del 1ro de mayo de 2017, la Sección Técnica de Grabaciones estaba adscrita a la División de Apoyo Técnico de la Superintendencia Auxiliar de Investigaciones Criminales (SAIC), de conformidad con la Orden General 100-107 del 1 de mayo de 2014. Posteriormente, con la Orden General 100-107 del 30 de junio de 2017 (sobre la "Reorganización de la Superintendencia Auxiliar en Investigaciones Criminales") se colocó formalmente a la Sección Técnica de Grabaciones bajo el Centro de Recopilación, Análisis, Diseminación de Inteligencia Criminal (CRADIC), a su vez adscrito a SAIC. Más recientemente, a través de la Orden General 100-134 de 30 de agosto de 2018, se estructuró el CRADIC (se mantuvo dentro de este a la Sección Técnica de Grabaciones) como un organismo adscrito y directamente responsable a la Oficina del Comisionado del Negociado de la Policía. Véase además, Orden General 100-102 del 13 de noviembre de 2018 (que estableció al CRADIC como una oficina adscrita a la Oficina del Comisionado).

Durante todo el periodo relevante a esta investigación, y durante los eventos del primero de mayo de 2017, las gestiones de la Sección Técnica de Grabaciones han estado reguladas por la Orden General 600-610 del 10 de febrero de 2014, sobre "Normas a Seguir para la Grabación de Eventos Públicos". Más recientemente, esta Orden General fue revisada mediante la Orden General 600-610 del 20 de junio de 2018, sobre la "Grabación de Eventos Públicos". A continuación se detallan las funciones de los componentes institucionales relevantes así como los elementos de esta normativa sobre la grabación de eventos públicos.

Más allá de estos datos básicos, es importante destacar los parámetros de acción de esta Sección Técnica de Grabaciones, según la Orden General vigente para todo el periodo relevante a esta Investigación, es decir la Orden General 600-610 del 10 de febrero de 2014, sobre "Normas a Seguir para la Grabación de Eventos Públicos". Como se ha dicho, esta fue eventualmente enmendada, el 20 de junio de 2018. Por el momento, analizamos la Orden anterior, toda vez que fue bajo la normativa vigente durante el periodo en que ocurrieron los hechos investigados.

Según la Orden General más reciente sobre el "Centro de Recopilación, Análisis y Diseminación de Inteligencia Criminal (CRADIC)", Orden General 100-134 de 30 de agosto de 2018, el CRADIC es responsable de

> recopilar, evaluar, analizar y diseminar toda la información criminal de las actividades relacionadas al narcotráfico y crimen organizado, armas ilegales y cualquier otra actividad delictiva.

Esta Orden General, a su vez, establece las cinco Secciones que le componen:

(1) Sección de Análisis de Inteligencia Criminal
(2) Sección Rastreo de Armas de Fuego
(3) Sección Técnica de Grabaciones
(4) Sección de Análisis de Trasiego de Drogas "Counter Drug"
(5) Sección de Análisis de Lavado de Dinero

En cuanto a la Sección Técnica de Grabaciones, se establece que:

> Esta Sección Técnica tendrá la responsabilidad de brindar asesoramiento y apoyo a todas las unidades investigativas y sus componentes adscritos a la SAIC, así como a cualquier otra unidad del NPPR, en la obtención de grabaciones de imágenes digitales. Estas grabaciones podrán ser utilizadas como evidencia obtenida de sistemas de cámaras de seguridad en torno a las distintas escenas del crimen, y como los servicios solicitados de grabación de eventos públicos, según dispuesto en la Orden General Capítulo 600 Sección 610 titulada: "Grabación de Eventos Públicos". Además, grabará la rueda de identificación de voz conforme a la Orden General 600-640, titulada "Identificación del

Sospechoso" y la jurisprudencia establecida por el Tribunal Supremo de Puerto Rico: *Pueblo v. Hernández*, 175 D.P.R. 274 (2009).

La sección de técnicas de grabaciones de las siguientes Áreas Policiacas responderá operacionalmente al Director del CRADIC:

a. San Juan;
b. Humacao;
c. Ponce; y
d. Aguadilla

Según informado por la Policía, la Sección Técnica de Grabaciones cuenta con 15 cámaras de video digital, marca Panasonic, Modelo HV-180,[67] y se afirmó que "no existen cámaras que graben en un medio no digital".[68] Se informó además que, para las actividades del 1ro de mayo de 2017, de la Sección Técnica de Grabaciones estuvieron en funciones nueve (9) agentes, un (1) Sargento y un (1) Teniente.

Para propósitos de la Orden General de 2014 los "eventos públicos" son "actividades de interés general de la comunidad, que incluyen pero sin limitarse a reuniones multitudinarias, demostraciones, huelgas y protestas. Así también, se permitirán las grabaciones de video para otros propósitos autorizados por la Policía de Puerto Rico, como investigaciones confidenciales o de encubiertos, para la investigación de la escena de un crimen, entre otros."[69] Por tratarse de una Orden General muy escueta, y por su importancia en esta investigación, se citan sus partes relevantes de forma íntegra, destacando aquellas disposiciones que atienden los siguientes renglones: (1) lugares en que se permite la grabación; (2) las personas

[67] Contestación al tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 4.
[68] Id. Inciso 7.
[69] Orden General 600-610, de 10 de febrero de 2014, "Normas a seguir para la Grabación de Eventos Públicos", Parte I(C).

autorizadas para realizar las grabaciones; (3) la existencia de aviso público sobre el hecho de la grabación; (4) almacenaje, acceso y conservación del material grabado; (5) controles administrativos; (6) estructuras de supervisión; (7) reglamentación del uso del material grabado.

Primero, en cuanto a *los lugares en que se pueden grabar eventos*, se establece que:

> E. Los miembros de la Policía de Puerto Rico podrán grabar eventos públicos realizados en propiedades públicas donde los ciudadanos no tengan expectativa de intimidad. En las propiedades privadas, podrán hacerlo en justo balance entre el derecho a la intimidad que pueda tener la persona, y la protección de la vida y de la propiedad. Además, los miembros de la Policía de Puerto Rico están autorizados a grabar cualquier conducta que un ciudadano intencionalmente realice en público. Por ende, la grabación de dicha conducta está autorizada por esta orden general. Sin embargo, no se podrán realizar grabaciones en propiedades privadas, incluyendo los interiores (como por ejemplo, casas y negocios), salvo que estén presentes algunas de las excepciones al requisito de órdenes de allanamiento o haber obtenido dicha orden.

Conforme a esta disposición, se autorizaba la grabación de personas en lugares públicos, sujeto a que no haya una expectativa razonable de intimidad. La grabación en propiedades privadas está sujeta a un ambiguo e impreciso mandato de "justo balance entre el derecho a la intimidad que pueda tener la persona, y la protección de la vida y de la propiedad".

Segundo, en torno a las *personas autorizadas para realizar las grabaciones*, la Orden General establecía una prohibición de que se utilizaron equipos privados, o cualquier otro equipo no autorizado, para realizar grabaciones, o que las realizaron agentes no autorizados:

F. En todo momento los miembros de la Policía de Puerto Rico deben obtener autorización previa del Superintendente, del Superintendente Asociado o del Superintendente Auxiliar de Operaciones Estratégicas o su designado, para grabar eventos públicos.

G. Únicamente los miembros de la Policía de Puerto Rico asignados a la Unidad Técnica de Grabaciones estarán autorizados a grabar ciudadanos y eventos públicos. Solamente el equipo de grabación, propiedad y mantenimiento por la Policía de Puerto Rico puede ser utilizado para la grabación de ciudadanos y eventos públicos. Los miembros individuales de la Policía de Puerto Rico asignados a preservar el orden en eventos públicos, no están autorizados a grabar ninguna porción del evento utilizando equipos de grabación privados; incluyendo, pero sin limitarse a celulares y cámaras de video digitales. Antes de asignárseles equipo de grabaciones a los miembros de la Policía de Puerto Rico, el supervisor de la Unidad Técnica de Grabaciones se asegurará que dicho miembro conozca y tenga copia de esta orden general.

Tercero, la Orden General no contenía una expresión afirmativa de realizar un *aviso público sobre el hecho de la grabación*, cuando ocurriera. Así, se disponía:

I. No se ocultará de manera activa que un evento público se esté grabando bajo esta orden.

Cuarto, en cuanto al *almacenaje, acceso y conservación del material grabado*, se establecía:

O. Los DVD que almacenan grabaciones de actividad delictiva se conservarán de acuerdo a lo requerido por los Tribunales. Sin embargo, los DVD que no contengan actividad delictiva, se conservarán por un término de dos (2) años, contados a partir de la fecha que se realizó la grabación, salvo que formen parte de una investigación administrativa, judicial o legislativa. El proceso de la disposición de las grabaciones será establecido por el Superintendente.

En este sentido, el almacenaje de los videos grabados podía ser por tiempo indefinido si se determinaba que contenían "actividad delictiva", o si formaban parte

de alguna investigación o procedimiento judicial o administrativo. De lo contrario, se disponía que podían borrarse al cabo de los dos años de haberse grabado.

Quinto, a la Orden General entonces vigente contenía una serie de *controles administrativos*, por vía de la confección de informes y otros registros de eventos relevantes, como por ejemplo:

> K. Todas las vídeo grabaciones tomadas por un miembro de la Policía de Puerto Rico autorizado por esta Orden General, serán almacenadas por la Unidad Técnica de Grabaciones. Una vez finalice la grabación de video, el equipo de grabación y la tarjeta de almacenaje se llevarán a la Unidad Técnica de Grabaciones para su descarga. El miembro de la Policía de Puerto Rico que utilice el equipo de grabación, será responsable de preparar un informe en el que hará constar la fecha, hora, lugar y un resumen de lo grabado. Dicho miembro deberá indicar su nombre y número de placa, además del nombre y número de placa del supervisor que monitoreó la grabación. Un miembro de la Unidad Técnica de Grabaciones, debidamente adiestrado, sustraerá lo grabado y lo quemará en un "Digital Video Disc" (DVD), que será almacenado en las oficinas de la Unidad Técnica de Grabaciones. El supervisor de la Unidad de Grabaciones será responsable de verificar que las imágenes fueron grabadas correctamente antes de autorizar a borrar la totalidad de las imágenes grabadas durante el evento público.
>
> L. Una vez descargada la grabación, el miembro de la Unidad Técnica de Grabaciones va a rotular el DVD, con su nombre y número de placa del operador del equipo de grabación, con la fecha de la grabación, el nombre y placa del supervisor en la escena y el número de identificación de dicho DVD. Se le dará entrada el DVD en la bitácora de grabaciones y se conservará en la bóveda de seguridad designada en la Superintendencia Auxiliar de Operaciones Estratégicas.
>
> P. El Supervisor de la Unidad Técnica de Grabaciones será responsable de realizar inspecciones mensuales para corroborar a seguridad y el inventario de los DVD y vendrá obligado a someter un reporte mensual de los hallazgos al Superintendente Auxiliar de Operaciones Estratégicas, y éste a su vez al Superintendente. Dicho supervisor se asegurará que lo miembros de la Policía de

Puerto Rico entiendan y que cumplan con los procesos establecidos cuando utilicen equipo de grabaciones.

Sexto, en cuanto a las *estructuras de supervisión* establecidas por la Orden General para las grabaciones, se planteaba lo siguiente:

H. Toda grabación será supervisada y directamente monitoreada por el oficial de mayor rango en la escena.

J. Los miembros de la Policía de Puerto Rico deberán notificar a sus supervisores de manera inmediata cualquier desperfecto o mal funcionamiento del equipo de grabación, para que la acción correspondiente se tome, además deberán documentar dicho suceso en el reporte de grabación.

Séptimo, y último, la Orden General contenía tres disposiciones dirigidas a *regular el uso del material grabado* por parte de los funcionarios del Estado.

M. Queda totalmente prohibido, grabar, reproducir, colgar en Internet, transferir a equipos digitales, revisar el contenido de las grabaciones en su totalidad o cualquier porción, sin la debida autorización del Superintendente o su designado.

N. Toda grabación realizada por miembros de la Policía de Puerto Rico autorizados en esta orden general solamente podrá ser utilizada para evaluar la conducta y desempeño de los Agentes de la Policía, investigaciones criminales y en procedimientos administrativos, judiciales o legislativos.

Q. Toda solicitud interna o externa para revisar o distribuir una grabación en particular, tendrá que ser aprobada por el Superintendente o su representante designado. Los originales de los DVD serán conservados en la Superintendencia Auxiliar de Operaciones Estratégicas y será responsabilidad de la Unidad Técnica de Grabaciones producir las copias para la revisión y distribución de las grabaciones, a menos que el original sea requerido por el Tribunal.

Los parámetros establecidos en esta Orden General presentaron a esta Comisión unas interrogantes fundamentales sobre las garantías necesarias para la protección de

los derechos humanos, como los derechos de libertad de expresión, asociación e intimidad, así como, los riesgos de la selectividad en la vigilancia y sus consecuencias. La Comisión se planteó cuestiones tales como:

- qué controles se proveen institucionalmente para acceder a los videos grabados;
- qué funcionarios tienen autorización para acceder a los materiales grabados y bajo qué circunstancias se remueven o editan videos de los archivos de la Policía;
- qué criterios se utilizan para determinar cuáles actividades públicas grabar, y quién toma esta decisión;
- qué controles existen para determinar si existen múltiples copias de los videos y en qué lugares se encuentran o archivan los videos;
- cuál es la capacidad tecnológica y la potencia del equipo utilizado, para determinar el alcance del mismo a áreas con expectativa de intimidad;
- cuánto se descansa en la nueva tecnología de información para realizar grabaciones de eventos públicos (como, por ejemplo, el uso de "drones", tecnología de reconocimiento facial, "dash cams", o "body cams");
- en caso de que se utilicen estas tecnologías adicionales, qué parámetros existen para su uso.

A la luz de lo anterior, la Comisión recibió información de cuatro requerimientos a la Policía sobre aspectos relacionados, realizó una Inspección Ocular en las oficinas de CRADIC para indagar sobre estos asuntos y, además, sostuvo una reunión con el Sr. Arnaldo Claudio, Asesor Técnico de Cumplimiento para el caso

judicial federal bajo el cual a la Policía se le requiere revisar sus prácticas y sus políticas, entre otras fuentes.

Los hallazgos emanantes de estas gestiones investigativas se resumen a continuación, y se dividen en seis asuntos relacionados a la garantía de varios derechos constitucionales fundamentales: (1) falta de controles administrativos apropiados; (2) vulnerabilidad de los videos a ser editados o borrados selectivamente; (3) preocupación sobre el uso y adquisición de equipo apropiado, particularmente lo relacionado con nueva tecnología para grabar y analizar video; (4) falta de claridad en cuanto a los criterios para determinar qué actividad o evento se grabará; (5) riesgos de selectividad en la grabación de personas participantes de eventos públicos; (6) riesgo potencial de uso de compañías privadas por parte de agencias gubernamentales, fuera de la Policía de Puerto Rico. Como se ha dicho, algunos asuntos han sido abordados por una Orden General 600-610 enmendada (el 20 de junio de 2018), pero por el momento nos centramos en las prácticas utilizadas y en la normativa vigente durante el periodo bajo investigación.

(1) En términos de los *controles administrativos*, en varios momentos se preguntó a la Policía sobre la existencia de algún registro, bitácora o cualquier tipo de récord sistemático sobre las actividades que se graban,[70] no se nos brindó tal información.[71] Tampoco existen auditorías internas sobre las grabaciones que se recopilan; nuevamente remitiéndonos a los procedimientos que se instaurarían en el

[70] Segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, incisos 6(b) y 6(d).
[71] Contestación al segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, inciso 6.

futuro.[72] Asimismo, no existió durante todo el periodo bajo evaluación un registro de los oficiales asignados a cada tarea o evento, indicándose que eso es "parte de los planes de trabajo" de la Sección,[73] ni tampoco un informe del agente por cada evento grabado destacando los datos básicos de la gestión. Aunque es un asunto que con la Orden General nueva está supuesto a atenderse,[74] "en general lo que se hace es que la grabación se pasa a un disco DVD y se certifica y se entrega al investigador".[75]

Sobre este aspecto, es pertinente notar los señalamientos del Asesor Técnico de Cumplimiento, en torno a los videos del 1ro de mayo de 2017 captados por la Sección Técnica de Grabaciones. En su informe, encontró deficiencias en el sistema de archivo de los videos toda vez que su numeración, usualmente generada secuencialmente por las cámaras de video, reflejaba archivos omitidos (números ausentes de la secuencia), lo cual arroja dudas en torno a si finalmente se guardaron todos los videos captados y, por ende, en torno a la selectividad del material preservado.[76] Sobre este asunto, el informe del Asesor Ténico destacó:

> eight DVDs provide multiple video segments which are identified with the sequence number that the video recorder device has assigned to each of them. Two of these eight DVDs are missing several video segments according to the sequence number that the video recorder device assigned to all the segments. These facts cast doubts on the video

[72] Segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, incisos 6(f) y 6(g); Contestación al requerimiento, inciso 6.
[73] Segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, inciso 6(j); Contestación al requerimiento, inciso 6.
[74] La nueva Orden General contiene un formulario preparado con estos fines.
[75] Segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, inciso 6(q); Contestación al requerimiento, inciso 6.
[76] *Assessment Report, Police of Puerto Rico's Response to the demonstrations and incidents involving the Capitol building, the "Centro para Puerto Rico" and the Worker's Day*, Office of the Technical Compliance Advisor to the Agreement for the Sustainable Reform of the Puerto Rico Police Department, Case 3:12-cv-02039, Document 712-1, Filed 01/26/18.

> recordings that were received, and it could be questioned if they represent only part of the incidents recorded that day by CRADIC.[77]

Esta Comisión solicitó y obtuvo acceso a los videos por parte del Asesor Técnico de Cumplimiento, y pudo corroborar lo expuesto en el informe antes citado.

(2) En cuanto a la *vulnerabilidad de los videos a ser editados o borrados selectivamente*, el mencionado Informe del Asesor Técnico planteó esa posibilidad claramente. Por un lado, como se ha dicho, la política anterior contenía una norma de preservación e integridad del material: los videos debían ser mantenidos por un periodo de dos (2) años, luego de lo cual debían ser borrados, a menos que se determinara que contenían "actividad delictiva", o si formaban parte de alguna investigación o procedimiento judicial o administrativo. Actualmente, la nueva Orden General establece un término de preservación de cinco (5) años para videos que se identifiquen como que contienen actividad delictiva (o indefinido si son parte de un proceso judicial o administrativo), o de un (1) año si no contienen actividad delictiva, al cabo del cual deben borrarse.[78] **En ningún momento se hace mención en estas políticas a la posibilidad de borrar selectivamente material antes de los términos dispuestos, por razón alguna.**

Como planteó el Informe del Asesor Técnico:

> Section 610 of the General Order states that the DVDs that do not contain criminal activity, will be preserved for two (2) years, counting since the day that the recording was made, unless they are part of an administrative, judicial or legislative investigation. Any possible claim

[77] *Assessment Report, Police of Puerto Rico's Response to the demonstrations and incidents involving the Capitol building, the "Centro para Puerto Rico" and the Worker's Day*, Office of the Technical Compliance Advisor to the Agreement for the Sustainable Reform of the Puerto Rico Police Department, Case 3:12-cv-02039, Document 712-1, Filed 01/26/18. Pág. 7.

[78] Orden General 600-610 de 20 de junio de 2018, "Grabación de Eventos Públicos", Parte XI (3), Almacenamiento e Identificación de los Archivos.

> alleging that the missing video segments not provided to the TCA were deleted because they did not contain any criminal activity, would be a claim completely opposed to the mandates of Section 610 of the General Order[79].

No obstante, en la Inspección Ocular llevada a cabo en las oficinas de CRADIC se nos indicó que, cuando se somete el video grabado por los técnicos o agentes de la Sección Técnica de Grabaciones, en la División se borra o elimina el contenido que carece de importancia evidenciaria o que no revela información sobre la comisión de delitos. Se expresó, además, que después de esta revisión, y eliminación de contenido de ser necesario, es que se almacena contenido en los servidores. Al preguntársele a la Policía mediante un interrogatorio escrito sobre "los criterios específicos que se utilizan para determinar cuáles videos o porciones de videos borrar",[80] esta agencia contestó que "[e]l criterio para eliminar o 'borrar' videos de grabaciones es que no exista la comisión de delito."[81] Asimismo, se preguntó si los videos relacionados con las protestas del 1 de mayo de 2017 habían sido editados de alguna forma incluyendo, pero sin limitarse a, borrar contenido, modificar el orden de eventos captados, añadir videos de otras fuentes, la Policía contestó que "se edita toda actividad no criminal".[82] En cuanto a qué funcionario está a cargo de tomar la decisión sobre eliminar o preservar

---

[79] *Assessment Report, Police of Puerto Rico's Response to the demonstrations and incidents involving the Capitol building, the "Centro para Puerto Rico" and the Worker's Day*, Office of the Technical Compliance Advisor to the Agreement for the Sustainable Reform of the Puerto Rico Police Department, Case 3:12-cv-02039, Document 712-1, Filed 01/26/18. Pág. 10.

[80] Tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 2.

[81] Contestación al tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 2.

[82] Id. Inciso 27.

contenido,[83] se nos indicó que "[n]o existe un oficial específico designado por la PPR para efectuar dicho proceso de borrar contenido de una grabación".[84]

Resaltamos, además, los hallazgos del Informe del Asesor Técnico, toda vez que identificó al menos un grupo de videos que a todas luces fue sustancialmente editado. Ese informe describió porciones de videos que se entrelazaban entre sí de forma traslapada, de modo que por instantes se percibían y escuchaban simultáneamente ("transitions that depict different overlapping images").[85] Esta Comisión pudo corroborar la existencia de las ediciones planteadas en ese informe.

(3) En torno al *equipo utilizado por la Sección Técnica de Grabaciones*, como se ha dicho, la Sección Técnica de Grabaciones cuenta con 15 cámaras de video digital, marca Panasonic, Modelo HV-180.[86] Además se indicó que "no existen cámaras que graben en un medio no digital".[87] Esto último es relevante puesto que en el Informe del Asesor Técnico se expresa la posibilidad de que, durante las protestas del 1ro de mayo de 2017, se haya utilizado equipo obsoleto, como cámaras de cinta de video, y que se hayan reutilizado las cintas luego de grabarse en un DVD.[88] Este escenario, planteado por un funcionario que responde a la Corte de Distrito Federal para el Distrito de Puerto

---

[83] Tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 2.

[84] Contestación al tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 2.

[85] *Assessment Report, Police of Puerto Rico's Response to the demonstrations and incidents involving the Capitol building, the "Centro para Puerto Rico" and the Worker's Day*, Office of the Technical Compliance Advisor to the Agreement for the Sustainable Reform of the Puerto Rico Police Department, Case 3:12-cv-02039, Document 712-1, Filed 01/26/18. Pág. 8.

[86] Contestación al tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 4.

[87] Id. Inciso 7.

[88] Assessment Report, Police of Puerto Rico's Response to the demonstrations and incidents involving the Capitol building, the "Centro para Puerto Rico" and the Worker's Day, Office of the Technical Compliance Advisor to the Agreement for the Sustainable Reform of the Puerto Rico Police Department, Case 3:12-cv-02039, Document 712-1, Filed 01/26/18. Págs. 8-10.

Rico, presenta el riesgo del uso por la Policía de equipo de grabación no autorizado, carente de cualquier control o supervisión. Esta posibilidad es preocupante a la luz de las declaraciones de la Lcda. Mariana Nogales quien, en la Audiencia Pública del 11 de abril de 2018, explicó que—a base de su experiencia— ha visto a miembros de la uniformada grabar a personas con sus teléfonos móviles en reacción al hecho de que estuvieren grabando las acutaciones de la Policía.[89] Es importante destacar que el uso de cámaras personales está prohibido por la Orden General vigente durante el periodo investigado y por la aprobada en el 2018.

Durante la Inspección Ocular se pudo comprobar la adquisición por la Policía de Puerto Rico de varios "drones", vehículos aéreos no tripulados, sin que su uso esté regulado por esa agencia ya que no existe un protocolo ni una Orden General que atienda las particularidades de este tipo de tecnología. Específicamente se nos informó que: "La PPR posee uno (1). No utilizado el 1ro de mayo de 2017. Pendiente a ser utilizado por primera vez toda vez que aún no han sido utilizados los correspondientes permisos para su uso" por la Federal Aviation Administration (FAA).[90] Es importante notar que en su Inspección Ocular a las oficinas de CRADIC, esta Comisión pudo observar la existencia de **al menos cuatro (4) "drones"** (no uno, como incorrectamente se nos informó por escrito), equipados con cámara de grabación. Se pudo constatar en la Inspección Ocular del 16 de febrero de 2019 que la Policía de Puerto Rico adquirió estos "drones" aproximadamente un año antes. Se observó, además, que se trata de

[89] Tercera Audiencia Pública llevada a cabo el 11 de abril de 2018 en la Comisión de Derechos Civiles.
[90] Contestación al tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 17.

equipos marca DJI, Modelo Phantom 3 Standard, los cuales—según el manual de operación—tienen la capacidad de elevarse a 120 metros de altura y tienen una cámara digital capaz de girar 120 grados, 30 grados hacia arriba desde la posición frontal del equipo, hasta 90 grados vertical hacia abajo.[91] Este equipo tiene la capacidad de grabar en áreas claramente cobijadas por una expectativa razonable de intimidad, como sería el caso de observar a través de ventanas en edificios residenciales. No hay reglamentación especial en la Policía que atienda los retos específicos que esta tecnología presenta, al preguntar sobre este particular, sólo se nos remitió a la Orden General sobre grabación de eventos públicos ya mencionada.[92]

Finalmente, se preguntó específicamente sobre el uso de tecnología para analizar las imágenes, como, por ejemplo, tecnología de reconocimiento facial.[93] Aunque se contestó en la negativa, la Policía indicó que la Orden General (entonces borrador) sobre CRADIC contiene un lenguaje para contemplar el uso de este tipo de tecnología ("este inciso se hizo pensando en el futuro").[94] En lenguaje en cuestión establece que "[El Director del CRADIC]…[a]nalizará la información mediante el uso de los programas de computadoras (software), especialmente diseñados para estos fines".[95]

---

[91] Manual de Operación Phantom 3 Standard, disponible a través de https://www.dji.com/pr/phantom-3-standard.; https://dl.djicdn.com/downloads/phantom_3_standard/20170623/Phantom+3+Standard+User+Manual+v1.4.pdf

[92] Contestación al tercer requerimiento de información "Habeas Data" con fecha de 9 de abril de 2018, contestado el 30 de abril de 2018, inciso 18.

[93] Segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, inciso 6(l).

[94] Contestación al segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, inciso 6.

[95] Orden General 100-134 de 30 de agosto de 2018, "Centro de Recopilación, Análisis y Diseminación de Inteligencia Criminal (CRADIC), Parte III(2)(p).

(4) Por otra parte, destacamos la *falta de claridad en cuanto a los criterios para determinar qué actividad o evento se grabará.* Esta Comisión obtuvo diversas respuestas sobre este particular. De un lado, al preguntarse específicamente sobre los criterios que se utilizan para peticionar que determinado evento sea grabado, se nos planteó por escrito "La sana discreción del Comisionado, Véase Orden General 600-610, inciso F" (refiriéndose a la orden anterior estableciendo que "los miembros de la Policía de Puerto Rico deben obtener autorización previa del Superintendente, del Superintendente Asociado o del Superintendente Auxiliar de Operaciones Estratégicas o su designado, para grabar eventos públicos.")[96] Al mismo tiempo, se nos planteó que "de grabarse algún evento, dicho evento se graba en su totalidad durante el evento en particular, hasta que culmine el evento".[97] No obstante estas representaciones, durante la Inspección Ocular en las oficinas de CRADIC se planteó a esta Comisión que la decisión de grabar un evento respondía a una determinación de si hay riesgo de que acontezcan "actos criminales o violaciones de derechos civiles". Lo anterior revela una amplia discreción, y por ende, potencial de selección carente de criterios manejables, para determinar qué eventos, personas o actividades serán vigiladas por el Estado.

Se percibe, por tanto, una ausencia de parámetros reglamentarios y, además, estructuras procesales y administrativas que definan claramente lo que será observado y grabado. Al menos uno de los videos de las grabaciones del 1ro de mayo de 2017, proporcionados por el Asesor Técnico, presenta un ejemplo de estas posibilidades. Un

[96] Contestación al segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, inciso 9.
[97] Id. Inciso 11.

agente asignado a grabar desde la estación de Bomberos en Hato Rey, se trasladó motu proprio a otra localidad en la Avenida Muñoz Rivera (a la altura del Centro Judicial de San Juan), sin autorización previa de su supervisor. A este agente, **mientras está grabando**, se le escucha informar por teléfono a un Teniente a cargo de este cambio, y al mismo tiempo pidiendo autorización, estando ya en el nuevo lugar. Aunque no podemos constatar si la llamada telefónica en efecto ocurrió (no se puede escuchar el otro lado de la conversación) o si fue un parlamento diseñado para registrar el cambio, lo cierto es que el traslado de lugar ocurrió sin permiso.[98] Si un agente, durante el transcurso de un evento, tiene la discreción de decidir qué áreas cubrir y cuáles no, estarán abiertas las puertas a la arbitrariedad.

Dicho esto, también corroboramos que en tiempos recientes la Sección Técnica de grabaciones ha estado sumamente activa, tomando en cuenta la actividad de protesta en el contexto presente. En la Audiencia Pública del 11 de abril de 2018, la Lcda. Mariana Nogales testificó sobre diversas actividades de protesta a las que ella y un grupo de abogadas y abogados acuden de manera preventiva para ayudar y asesorar a manifestantes, en caso de que se produzcan arrestos u otras situaciones con la Policía. La Lcda. Nogales estableció que, durante el año 2017 y hasta abril de 2018, el grupo ha asistido a aproximadamente 2 actividades de protesta al mes (cerca de 30 manifestaciones), de diversos tamaños. Al preguntársele si, en su experiencia, "¿hay actividades que *no* están siendo grabadas?", contestó secamente: "Ni una". Lo anterior

[98] Disco Compacto Digital (DVD) marcado con el número 9, de los provistos por la Oficina del Asesor Técnico luego de ser solicitados por la Comisión como parte de los trabajos de investigación de la querella objeto de este informe; minuto 11:27.

(así como nuestras impresiones luego de estudiar el expediente de esta Investigación) nos hace pensar que la Unidad Técnica de Grabaciones es una fuerza especializada dirigida en gran medida (aunque no exclusivamente) a grabar manifestaciones de protesta política y social.

(5) Los hechos investigados también revelan ciertos riesgos con la *selectividad en la grabación de personas participantes de eventos públicos*. Expresamente se preguntó a la Policía de Puerto Rico si el CRADIC "mantiene un récord de los sujetos u organizaciones que aparecen en estas grabaciones", contestándose lo siguiente:[99]

> No se mantienen registro de individuos, en borrador de la Orden tampoco hace referencia a algún registro de individuos. Es importante aclarar que la Sección Técnica de Grabaciones no entra en el contenido de la grabación. Su función es grabar el evento y remitir la grabación al agente investigador (que no pertenece al CRADIC) para que continúe con la investigación criminal que está realizando. Por lo tanto, CRADIC no crea ninguna carpeta de ningún individuo, de hecho, tampoco identifica individuos u organizaciones en los videos realizados. El Centro tiene la responsabilidad de mantener custodia, control y confidencialidad de toda la información recibida de organizaciones criminales en Puerto Rico.[100]

Esta postura de neutralidad da al traste con algunos de los hechos observados. Por ejemplo, en videos examinados de las protestas del 1ro de mayo de 2017 se ve que el agente acercó el tiro de la cámara (mediante el *zoom* del lente) hacia personas en particular por un tiempo sustancial (en lugar de grabar tiros amplios de los eventos). Algunas de estas personas tenían sus rostros tapados, otras no. En una ocasión se hizo un esfuerzo por alcanzar a tomar (y así se escuchó decir al agente) la tablilla de un

---

[99] Segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, inciso 6(e).

[100] Contestación al segundo requerimiento de información "Habeas Data" con fecha de 3 de noviembre de 2017, contestado el 12 de diciembre de 2017, inciso 6.

vehículo de motor tipo "pick up", donde estaban unas personas de aparente interés para el agente tomando agua.[101] Debe notarse que estas personas, como muchas otras en la manifestación, tenían sus rostros tapados lo cual no era, ni es actualmente, un acto delictivo en si mismo (a no ser que se haga para encubrir la comisión de algún delito).[102]

(6) Finalmente, se alertó a esta Comisión sobre el riesgo potencial del *uso de compañías privadas por parte de agencias gubernamentales*, fuera de la Policía de Puerto Rico. Este asunto fue planteado mediante carta del 11 de abril de 2018 por el Representante Denis Márquez Lebrón. En su comunicación, y según reiteró en Audiencia Pública de esa misma fecha, explicó que el 26 de marzo de 2018 –durante una protesta frente a las oficinas del Departamento de Trabajo de Puerto Rico— presenció "cómo personas que aparentaban ser empleadas de alguna compañía contratada por el DTRH comenzaron a grabar a los manifestantes desde el edificio". La Policía de Puerto Rico, mediante contestación escrita, negó conocer sobre gestiones de vigilancia y grabación con contratistas privados,[103] aunque estuvo presente en dicho evento. Esta Comisión no tiene evidencia para concluir que la Policía esté incurriendo

---

[101] Disco Compacto Digital (DVD) marcado con el número 9, de los provistos por la Oficina del Asesor Técnico luego de ser solicitados por la Comisión como parte de los trabajos de investigación de la querella objeto de este informe; minuto 8:29.

[102] El artículo 248 del Código Penal establece:

> Incurrirá en delito menos grave, toda persona que utilice una máscara o careta, postizo o maquillaje, tinte, o cualquier otro disfraz, completo o parcial, que altere de cualquier forma temporera o permanentemente su apariencia física con el propósito de:
> (a) Evitar que se le descubra, reconozca o identifique en la comisión de algún delito.
> (b) Ocultarse, evitar ser arrestado, fugarse o escaparse al ser denunciado, procesado o sentenciado de algún delito.
> (c) Alterar o intervenir con las actividades ordinarias en una instalación pública educativa, en una instalación de salud, o en el interior de edificios de gobierno.

Debe notarse que el 19 de mayo de 2017 el artículo 248 del Código Penal fue enmendado, manteniendo la prohibición para estos caos que existía en el atículo 248 a la fecha de estos hechos. Véase Ley 27 de 19 de mayo de 2017, sección 15.

[103] Contestación al cuarto requerimiento de información "Habeas Data" con fecha de 26 de abril de 2018, contestado el 2 de mayo de 2018, inciso 7.

en esta práctica, subcontratando estas tareas. No obstante, se registra este hecho como un área de preocupación fuera del alcance de este informe: la posibilidad de un sistema paralelo de grabación gubernamental, motivado por agencias gubernamentales, llevado a cabo por empresas de seguridad contratadas.

Algunas de las áreas de preocupación aquí señaladas puede que estén atendidas por nuevas Órdenes Generales sobre el particular. Así por ejemplo, la Orden General 600-610 del 20 de junio de 2018, sobre la Grabación de Eventos Públicos, contiene disposiciones sobre: (a) la grabación íntegra e ininterrumpida de un evento; (b) prohibición de "grabaciones selectivas hacia grupos o personas particulares mientras estos estén en un ejercicio legítimo de su derecho constitucional de expresión"; (c) requisito de adiestramiento y recertificación cada dos años del personal autorizado a grabar; (d) auditorías e inspecciones al azar del material preservado en los servidores; (e) requisitos para la identificación y registro de la evidencia digital previo a su almacenamiento en servidores; (f) requisito para que las grabaciones se mantengan inéditas, entre otras.

Si bien estos cambios representan un adelanto significativo y bienvenido, también es cierto que las preocupaciones antes señaladas se manifestaron en el contexto de la Orden General del 2014 que también imponía ciertos requisitos. Así, por ejemplo, la edición de videos y la práctica de borrar contenido discrecionalmente, ocurrió ante un mandato reglamentario de preservar los materiales por un periodo de dos años. La adquisición y la intención de uso de varios equipos de vigilancia ("drones"), sin mediar guías claras para su uso y para la protección de derechos constitucionales (aparentemente descansando en una Orden sobre grabaciones pensada para otro tipo de

tecnología), es particularmente preocupante. El aparente uso de cámaras personales por agentes de ley y orden (no del CRADIC) para grabar a ciudadanos, según testificado en audiencia pública, se da en contraste a una prohibición expresa para ello en la Orden previa. La ausencia de registros, récords, informes u otros mecanismos de control (necesarios para salvaguardar la integridad del material grabado y evitar su manipulación), ocurrió durante la vigencia de un requisito expreso en la Orden General anterior de que el agente que utilice el quipo de grabación "será responsable de preparar un informe en el que hará constar la fecha, hora, lugar y un resumen de lo grabado". Ante este cuadro, las nuevas directrices—aunque pueden presentar un buen paso—no pueden percibirse como suficientes ante lo que, a todas luces, es una cultura institucional que no es conducente a la protección de derechos en este contexto.

D. El uso de otra tecnología de información en la Policía de Puerto Rico para fines investigativos

Según se desprende de la discusión anterior, durante el transcurso de esta investigación encontramos el interés de la Policía de Puerto Rico de utilizar desarrollos tecnológicos al servicio de sus funciones investigativas. En este sentido, hemos descrito (a) el uso de tecnología –mediante la presencia en redes sociales—para complementar las técnicas de investigación de la Policía; (b) la adquisición (prematura) de "drones" por la Sección Técnica de Grabaciones y (c) la inclusión de lenguaje en la Orden Ejecutiva que estructura al CRADIC "pensando en el futuro", mencionada cuando se preguntó a la Policía sobre el posible uso de tecnología de reconocimiento facial. Asimismo, en la Inspección Ocular al CRADIC se mencionó el uso de "License

Plate Readers", tecnología que detecta los números de las tablillas de vehículos de motor para contrastar con bases de datos sobre vehículos hurtados. En el panorama se encuentran técnicas sofisticadas de análisis de información, ya sea visual o de otra clase, como por ejemplo, tecnologías de análisis predictivo e inteligencia artificial. En la medida en que los presupuestos de las agencias de ley y orden se ven contraídos, el uso de tecnologías de información sofisticadas puede verse lejano; al mismo tiempo, la promesa de que las tecnologías de información hacen de la gestión policíaca una potencialmente más eficiente y, a la larga, más costo efectiva, constituye un poderoso incentivo para experimentar y adoptar nuevos mecanismos.[104] Aunque este informe no pretende evaluar todas las dimensiones del aparato tecnológico de la Policía de Puerto Rico, sí se revelan hechos que levantan bandera sobre su potencial desarrollo futuro.

En particular, destacamos una entrevista que sostuvimos con el Dr. Juan Carlos Rivera Hernández, Director del Negociado de Tecnología Informática. Este Negociado tiene como responsabilidad principal la "planificación, organización, implantación y mantenimiento de los sistemas computadorizados de información y comunicaciones" de la Policía de Puerto Rico[105]. Entre las funciones del Director, está administrar "toda actividad relacionada a la adquisición de tecnologías requeridas por las Superintendencias incluyendo sus divisiones, secciones y unidades de trabajo en términos de sus necesidades operacionales y administrativas."[106] Asimismo, "velará porque todo [Miembro del Negociado de la Policía de Puerto Rico] esté debidamente

[104] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (2017).
[105] Orden General 100-123 del 25 de abril de 2018, "Negociado de Tecnología y Comunicaciones", Parte I. Propósito.
[106] Id. Parte III(A)(1).

adiestrado sobre la utilización de los sistemas de información"[107] y "[a]nalizará y someterá recomendaciones sobre las normas y procedimientos relacionados con los sistemas de tecnología y comunicaciones que se implanten".[108]

Ante el cuadro que hemos descrito, en torno al uso y adquisición de tecnología por la Policía de Puerto Rico, así como los diversos riesgos de potencial mal uso y abuso que cada una puede presentar desde una perspectiva de derechos humanos, resulta evidente para esta Comisión que toda decisión sobre la adquisición de nueva tecnología debe estar precedida de un análisis de su potencial impacto sobre el disfrute de derechos. Asimismo, es necesario que—por cada tecnología en planes de adquisición—se desarrollen políticas apropiadas y planes de adiestramientos que ayuden a limitar los riesgos de que se afecten los derechos de las personas. En este sentido, el Negociado de Tecnología Informática tiene un rol institucional importante que jugar en la evaluación de estas tecnologías y en la evaluación del impacto sobre los derechos humanos. Pero en una oficina con tres empleados actualmente, de diez posibles posiciones, difícilmente esta tarea podrá materializarse efectivamente.[109]

La adquisición de costosos "drones" sin políticas, sin planificación, sin permisos, y sin adiestramiento debe servir como advertencia de lo que puede el futuro del uso y adquisición de tecnología de vigilancia, con un impacto previsible sobre los derechos constitucionales de las personas. Institucionalmente, el Negociado de Tecnología Informática (o alguna oficina como esta) debe cumplir una función de

[107] Orden General 100-123 del 25 de abril de 2018, "Negociado de Tecnología y Comunicaciones", Parte III(A)(7).
[108] Id. Parte III(A)(9).
[109] Reunión con Dr. Juan Carlos Rivera el 1ro de noviembre de 2018.

planificación de adquisición tecnología que evite estas posibilidades. No obstante, en el caso de los "drones" específicamente se trató de una adquisición que no pasó por esta oficina.[110] Lo anterior denota falta de integración entre el Negociado de Tecnología Informática y otros componentes de la Policía. El objetivo que encierra el aforismo "por cada nueva tecnología, una política apropiada" será inasequible si no existe esta integración y la asignación de recursos necesarios.

V. Determinaciones de Hechos

Analizados los documentos, los testimonios y la información recopilada durante las vistas, la Comisión hace las siguientes determinaciones de hechos:

A. Prácticas de monitoreo por parte de agentes de orden público en redes sociales

1. El 26 de abril de 2017, la entonces Superintendente de la Policía, Cor. Michelle Hernández de Fraley, emitió ciertas expresiones sobre el monitoreo en redes sociales por ese cuerpo. Entre sus expresiones se encuentran las siguientes: "[e]stamos monitoreando las redes sociales tenemos acceso a lo que se ha manifestado de las diferentes organizaciones" y que "todo el mundo postea [en Facebook] sus intenciones y nosotros monitoreamos esas intenciones y corroboramos que las intenciones son más que palabras"[111].
2. La entonces Superintendente tuvo la oportunidad de elaborar en torno al alcance de estas expresiones ante la Comisión de Derechos Civiles.[112] De su testimonio se desprende que la postura de la Policía de Puerto Rico ante la Comisión fue que esta agencia no monitorea afirmativamente a personas por razón de sus expresiones, sino que, en cambio, el monitoreo realizado en anticipo al primero de mayo de 2017 fue más bien reactivo—en respuesta a "mensajes y confidencias recibidas por

[110] Reunión con Dr. Juan Carlos Rivera el 1ro de noviembre de 2018.
[111] Meléndez, Lyanne, Policía verifica redes sociales de los manifestantes, Metro PR, 26 de abril de 2017, https://www.metro.pr/pr/noticias/2017/04/26/policia-verifica-redes-sociales-manifestantes.html
[112] En Audiencia Pública del 5 de julio de 2017.

ciudadanos sobre ataques, agresiones y amenazas días antes de la manifestación". Además, expresó que esta información se adquiere de elementos que están en redes sociales a plena vista, disponibles a otras personas.

3. En respuesta a un requerimiento de información del 30 de mayo de 2017, la Policía de Puerto Rico informó ante la Comisión que "no ha creado expedientes de personas y/o entidades como resultado de investigaciones en redes sociales".

4. La División de Crímenes Cibernéticos la encargada de evaluar conducta de personas a través de las redes sociales bajo el protocolo establecido en la Orden General Núm. 600-613, titulada "Normas para Solicitar, Monitorear, Intervenir y Procesar las Actividades Relacionadas a Crímenes Cibernéticos", del 29 de agosto de 2014, vigente al momento de los eventos del 1 de mayo de 2017.

5. La Orden General Núm. 600-613 entonces vigente específicamente establecía la autoridad de la División de Crímenes Cibernéticos de la Policía para "realizar monitoreos de las redes sociales" como una actividad fundamentalmente desregulada. Solamente luego de encontrarse actividad sospechosa en ciertos casos, actividad delictiva o tras recibirse la información por una fuente es que se activarían ciertos requisitos procesales.

6. La Orden General Núm. 600-613 carece de criterios para controlar la discreción otorgada a la Policía.

7. De conformidad con el testimonio de la Superintendente, así como el del Sargento Luis Maldonado, Director de Crímenes Cibernéticos, la Policía no realiza monitoreo motu proprio, sino que ello se produce en respuesta a confidencias e información recibida a través de un "Fan Page" de Facebook de la Policía.[113]

8. La Superitendente expresó que "no es la misión de [los agentes adscritos a la División de Crímenes Cibernéticos] estar haciendo eso", refiriéndose a la búsqueda proactiva de personas u organizaciones vinculadas a un evento multitudinario como la protesta del 1 de mayo de 2017, ya que "ese no es el comportamiento dentro de esta sección, la cual ha sido certificad[a] para hacer este trabajo."[114]

9. El Sargento Luis Maldonado indicó que esa División no utiliza programas de computadora para monitorear movimientos en redes

[113] Según surge de sus testimonios en Audiencia Pública del 5 de julio de 2017.
[114] Id.

sociales, no monitorean las redes sociales y no ha recibido instrucción alguna para monitorear redes.[115]

10. En contestación a requerimiento de información, la Policía de Puerto Rico informó que para los eventos del 1 de mayo de 2017 no se crearon expedientes relacionados con querellas presentadas o información recibida sobre expresiones en redes sociales. Es decir, aunque se indicó que el monitoreo en cuestión previo a las manifestaciones del 1ro de mayo de 2017 fueron motivados por mensajes y confidencias en redes sociales aparentemente conectadas con potenciales actos violentos, no se obtuvo evidencia de registro alguno de estas confidencias.

11. Por otro lado, la Policía proveyó información a esta Comisión de seis referidos realizados al *Federal Bureau of Investigation* (FBI) por expresiones en Facebook entre el 28 de abril y el 1 de mayo de 2017 luego de recibir confidencias en torno a alegadas amenazas a la seguridad pública. Más allá de esos referidos al FBI, no se abrió un expediente de estos incidentes potencialmente criminales en redes sociales que, se nos dice, motivaron el monitoreo digital por la Policía.

12. Los comentarios en Facebook reportados a la Policía y que ésta a su vez refirió al FBI fueron todos catalogados como "amenaza", y sobre ellos la Policía de Puerto Rico preservó los referidos al FBI. Una vez referidos estos casos al FBI, terminó el contacto de la Policía con ellos.

13. Al menos una de las personas referidas por la Policía de Puerto Rico al FBI por comentarios en Facebook, fue inmediatamente arrestada y acusada por las agencias federales de ley y orden por alegada violación a un delito federal de amenazas. Las acusación federal se realizó el 29 de abril de 2017, tan pronto como la Policía refirió el asunto al FBI por la persona expresar "Vamos a bombardear el Capitolio y que en paz descansen nuestras conciencias".

14. El mismo día de la acusación federal, dos días antes de los eventos del 1ro de mayo de 2017, la fiscal federal para el Distrito de Puerto Rico, Rosa Emilia Rodríguez, comunicó a todos los medios del país el arresto de esta persona, lo cual fue reseñado por todos los medios del país.

15. Si bien la Superintendente declaró que la Policía de Puerto Rico estuvo "monitoreando las redes sociales" sólo "en respuesta a los mensajes y confidencias recibidas por ciudadanos sobre ataques, agresiones y amenazas días antes de la manifestación", no brindó a esta Comisión información específica sobre estos "mensajes y confidencias recibidas por ciudadanos" que alegadamente activaron un monitoreo de redes sociales.

---

[115] Informado durante Inspección Ocular del 16 de febrero de 2018 a las facilidades de la División de Crímenes Cibernéticos en el Cuartel General de la Policía.

16. Aun si tomamos como cierta la palabra de la entonces Superintendente a los efectos de que en efecto hubo monitoreo de redes sociales durante la semana previa a las manifestaciones del 1ro de mayo de 2017, esta Comisión no tiene constancia de las razones que motivaron el monitoreo. Sí hay base para concluir que, cualesquiera hayan sido estas razones, no se trató de denuncias en redes sociales sobre conducta delictiva en esta jurisdicción.

17. La Comisión pudo constatar que la Policía refirió al FBI ciertas expresiones y comentarios en Facebook entre el 28 de abril y el 1 de mayo (posteriores a las expresiones de la Superintendente en los medios) sobre asuntos que la Policía se entiende sin jurisdicción y, en un caso, las agencias federales realizaron un arresto inmediato y denuncia (eventualmente desestimada), lo cual procuraron anunciar a todo el país justo antes de las manifestaciones políticas.

18. La Policía de Puerto Rico no proveyó información sobre perfiles, cuentas de redes sociales o páginas de internet de personas u organizaciones que han sido o actualmente están siendo monitoreadas por la PPR, alegando que dicha información no existe en el Negociado.

19. La Policía informó que no intervino, arrestó o citó a persona alguna como resultado de un monitoreo de redes sociales en el contexto de las protestas del 1ro de mayo de 2017. También indicó que la PPR no solicitó órdenes judiciales a un tribunal general de justicia producto del mencionado monitoreo. Tampoco proveyó lista de perfiles creados por la PPR para realizar su trabajo ya que adujeron su confidencialidad, pues se trata de investigaciones criminales en curso.

20. La División de Crímenes Cibernéticos de la Policía de Puerto Rico está adscrita a la Superintendencia Auxiliar en Investigaciones Criminal según la Orden General 100-102, "Estructura del Negociado de la Policía de Puerto Rico, del 13 de noviembre de 2018 y de conformidad con la Orden General 100-107, "Reorganización de la Superintendencia Auxiliar en Investigaciones Criminales", de 30 de junio de 2017.

21. Durante el transcurso de esta investigación, el 28 de abril de 2018, se aprobó una nueva Orden General 600-613, titulada "División de Crímenes Cibernéticos", para regular la misma División.

22. Esta División atiende entre 1,200 y 1,400 casos anuales, de los cuales aproximadamente 400 tienen que ver con conducta en redes sociales. La mayor parte de los asuntos atendidos se relacionan con situaciones de amenazas, violencia doméstica, acoso y asuntos similares.

23. La Orden General 600-613 del 20 de agosto de 2014 (vigente a la fecha de los eventos pertinentes) estableció que esta División fue creada para (a) "brindar apoyo técnico especializada a la rama investigativa tanto de las Áreas Policiacas como a nivel central"; (b) realizar "las

investigaciones donde requiera personal técnico especializado en el uso de equipo computadorizado"; así como (c) "detectar y esclarecer la actividad criminal mediante el uso de informática que incluye fraude electrónico, pornografía infantil, falsificación y acceso no autorizado".

24. La nueva Orden General 600-613 del 25 de abril de 2018, aprobada durante el transcurso de esta investigación, y que reemplaza la Orden vigente durante las protestas del 1ro de mayo de 2017, mantiene un lenguaje similar al antes descrito, pero reemplazando la norma de que la División "realizará monitoreos" con la frase "evaluará toda información recibida", en un aparente esfuerzo por rectificar la postura sobre el monitoreo proactivo recogida en la Orden anterior, pero negada a esta Comisión. Asimismo, la nueva Orden General establece en su Parte V(B)(1) que "se prohíbe a todo [Miembro del Negociado de la Policía de Puerto Rico] que, sin un fin legítimo, levante, mantenga, preserve, recopile información personal de individuos, organizaciones, agrupaciones, si dichos individuos, organizaciones y agrupaciones no están vinculados con la comisión o intento de cometer un delito.

B. *Prácticas de recopilación de información privada digital durante el ejercicio de funciones investigativas*

1. La Orden 600-613 del 29 de agosto de 2014 (vigente al momento de los eventos bajo investigación) que reglamenta la División de Crímenes Cibernéticos, adscrita a la Superintendencia Auxiliar de Investigaciones Criminales, establecía algunos elementos relacionados con la obtención de información privada almacenada en servidores de los servicios en internet utilizados por las personas.

2. Según la referida Orden, una vez se detecta conducta potencialmente delictiva, observada en redes sociales, la División de Crímenes Cibernéticos toma las siguientes acciones: (a) solicita a la plataforma de internet que preserve información relevante, toda vez que podrá ser solicitada como parte de un proceso investigativo; (b) coordina con el Ministerio Público (en particular la Unidad Investigativa de Crímenes Cibernéticos del Departamento de Justicia), la preparación y presentación de *subpoenas* u órdenes judiciales de registro para solicitar información, según aplique y (c) tramita el *subpoena* u orden de registro y recibe la información personal por parte de la plataforma digital, para su evaluación y análisis.

3. En cuanto al tipo de información solicitada, durante el transcurso de investigaciones relacionadas con conducta observada en las redes sociales, las agencias de orden público pueden solicitar información como la dirección de correo electrónico, la Dirección de Protocolo de Internet (Dirección IP), historial de uso de una persona de una red social

en determinado periodo de tiempo y el contenido de las comunicaciones en una red social o plataforma de internet.

4. Con la Dirección IP asociada a un usuario, el Estado a su vez puede obtener otra información por parte de otras entidades, en particular Proveedores de Servicio de Internet (ISP, por sus siglas en inglés).

5. Al menos un un Proveedor de Servicio de Internet (ISP, por sus siglas en inglés) al que esta Comisión tuvo la oportunidad de entrevistar aclaró que en el pasado se le ha solicitado información sobre el historial de visitas de un cliente (como, por ejemplo, qué páginas de internet visitó en determinado momento o en determinado periodo de tiempo). Ello es consistente con lo manifestado por el Director de la División de Crímenes Cibernéticos, Sgto. Maldonado, en Inspección Ocular en las oficinas de la División de Crímenes Cibernéticos. Al mismo tiempo, ese ISP indicó que, aunque se le ha solicitado la información, esta no es almacenada en sus sistemas por lo que es incapaz de proveerla.

6. La Orden 600-613 del 29 de agosto de 2014 no contiene descripción del tipo de información obtenible mediante requerimiento u orden judicial a plataformas de internet.

7. En cuanto al tipo de procedimiento utilizado para solicitar información personal que se encuentra alojada en los servidores de las plataformas de internet la Comisión indagó sobre si, por un lado, la información se solicita a través de una orden judicial o si, en cambio, es obtenida mediante un requerimiento no judicial de información, como lo es el *subpoena duces tecum* que emite el Gobierno sin supervisión de la Rama Judicial.

8. El entonces Director de la Unidad Investigativa de Crímenes Cibernéticos del Departamento de Justicia, el Fiscal Rafael Sosa, articuló las circunstancias en que el Departamento de Justicia solicita información almacenada digitalmente mediante orden y mediante *subpoena*.

9. Según informado a la Comisión, el Departamento de Justicia se deja llevar por el régimen federal para solicitar la información que es alojada en servidores de terceros: cuando se trata de información catalogada como transaccional (que no es contenido de comunicaciones) se solicita por medio de *subpoena*. Por otro lado, cuando se trata del contenido de una comunicación, siempre habrá que solicitarlo mediante orden judicial.

10. El Fiscal Sosa explicó que el Departamento de Justicia atempera los requerimientos al caso *Weber v. E.L.A.*, 190 D.P.R. 688 (2014), jurisprudencia que establece una protección mayor al derecho a la intimidad.

11. Esta Comisión solicitó al Departamento de Justicia en audiencia pública cualquier guía interna del Departamento que articule estos criterios de forma precisa. A pesar de que se informó que existían unas "guías de evidencia digital que se circulan a los fiscales" para ayudarles en estos procesos, e inicialmente se indicó en Audiencia Pública que se brindarían las mismas a esta Comisión, el Departamento de Justicia eventualmente se negó a bridar estas guías, a pesar de reiterados requerimientos.

12. La única fuente de información que arroja luz sobre estos elementos se encuentra en la nueva Orden General 600-613, aprobada el 25 de abril de 2018 mientras esta investigación estaba en curso. Dicha Orden contiene una nueva Parte I, estableciendo la Sección de Requerimientos Legales (o "Legal Requests") adscrita a la División de Crímenes Cibernéticos. Allí se establecen los parámetros para utilizar orden judicial o *supboena*.

C. *La grabación de actividades de protesta pública con cámaras de video y audio*

1. En términos organizativos, la división que está a cargo de grabar eventos públicos, así como de archivar el video grabado y mantener el equipo para ello, es la Sección Técnica de Grabaciones. La ubicación institucional de esta Unidad ha variado en los últimos años.

2. Durante todo el periodo relevante a esta Investigación, y durante los eventos del primero de mayo de 2017, las gestiones de la Sección Técnica de Grabaciones han estado reguladas por la Orden General 600-610 del 10 de febrero de 2014, sobre "Normas a Seguir para la Grabación de Eventos Públicos". Más recientemente, esta Orden General fue revisada mediante la Orden General 600-610 del 20 de junio de 2018, sobre la "Grabación de Eventos Públicos".

3. Según la Orden General más reciente sobre el "Centro de Recopilación, Análisis y Diseminación de Inteligencia Criminal (CRADIC)", Orden General 100-134 de 30 de agosto de 2018, el CRADIC es responsable de recopilar, evaluar, analizar y diseminar toda la información criminal de las actividades relacionadas al narcotráfico y crimen organizado, armas ilegales y cualquier otra actividad delictiva.

4. Esta Orden General, a su vez, establece las cinco Secciones que le componen: (1) Sección de Análisis de Inteligencia Criminal; (2) Sección Rastreo de Armas de Fuego; (3) Sección Técnica de Grabaciones; (4) Sección de Análisis de Trasiego de Drogas "Counter Drug"; (5) Sección de Análisis de Lavado de Dinero

5. En cuanto a la Sección Técnica de Grabaciones, la Orden General establece que brindará asesoramiento y apoyo a todas las unidades

investigativas y cualquier otra unidad del NPPR en la obtención de grabaciones de imágenes digitales. Establece además que dichas grabaciones podrán ser utilizadas como evidencia obtenida de sistemas de cámaras de seguridad en torno a las distintas escenas del crimen, y como los servicios solicitados de grabación de eventos públicos, según dispuesto en la Orden General Capítulo 600 Sección 610 titulada: "Grabación de Eventos Públicos", entre otras funciones.

6. La sección de técnicas de grabaciones de las Áreas Policiacas de San Juan, Humacao, Ponce y Aguadilla responden operacionalmente al Director del CRADIC.

7. Según informado por la Policía, la Sección Técnica de Grabaciones cuenta con 15 cámaras de video digital, marca Panasonic, Modelo HV-180, afirmándose que "no existen cámaras que graben en un medio no digital". Se informó además que, para las actividades del 1ro de mayo de 2017, de la Sección Técnica de Grabaciones estuvieron en funciones nueve (9) agentes, un (1) Sargento y un (1) Teniente.

8. Para propósitos de esa Orden General "eventos públicos" son "actividades de interés general de la comunidad, incluyendo pero sin limitarse a reuniones multitudinarias, demostraciones, huelgas y protestas. Así también, se permitirán las grabaciones de video para otros propósitos autorizados por la Policía de Puerto Rico, como investigaciones confidenciales o de encubiertos, para la investigación de la escena de un crimen, entre otros."

9. En cuanto a los lugares en que se pueden grabar eventos, en la Orden General se autoriza la grabación de personas en lugares públicos, sujeto a que no haya una expectativa razonable de intimidad. La grabación en propiedad privada está sujeta a un ambiguo e impreciso mandato de "justo balance entre el derecho a la intimidad que pueda tener la persona, y la protección de la vida y de la propiedad".

10. En torno a las personas autorizadas para realizar las grabaciones, la Orden General establecía una prohibición de que se utilicen equipos privados (o cualquier otro equipo no autorizado) para realizar grabaciones, o que graben agentes no autorizados. Únicamente los miembros de la PPR asignados a la Unidad Técnica de Grabaciones estarán autorizados a grabar ciudadanos y eventos públicos.

11. La Orden General no contenía una existencia robusta de aviso público sobre el hecho de la grabación, cuando ocurriera. Así, se disponía: "No se ocultará de manera activa que un evento público se esté grabando bajo esta orden".

12. En cuanto al almacenaje, acceso y conservación del material grabado, se establecía que los DVD que almacenan grabaciones de actividad delictiva se conservarán de acuerdo a lo requerido por los Tribunales.

Sin embargo, los DVD que no contengan actividad delictiva, se conservarán por un término de dos (2) años, contados a partir de la fecha que se realizó la grabación, salvo que formen parte de una investigación administrativa, judicial o legislativa.

13. El almacenaje de los videos grabados de acuerdo a la Orden podría ser indefinido si se determinaba que contienen "actividad delictiva", o si forman parte de alguna investigación o procedimiento judicial o administrativo. De lo contrario, se disponía para ser borrados en dos años de haberse grabado.

14. La Orden General entonces vigente, dispuso para una serie de controles administrativos, por vía de la confección de informes y otros registros de eventos relevantes. Las grabaciones en video tomadas por un miembro de la PPR son almacenadas por la Unidad Técnica de Grabaciones y se establece un protocolo para preservar el tracto de la grabación.

15. En cuanto a las estructuras de supervisión establecidas por la Orden General para las grabaciones de la Sección, se planteaba que toda grabación será supervisada y directamente monitoreada por el oficial de mayor rango en la escena.

16. La Orden General contenía tres disposiciones dirigidas a regular el uso del material grabado por parte de los funcionarios del Estado: (1) no se puede grabar, reproducir, colgar en Internet o reproducir el contenido de las grabaciones sin la debida autorización del Superintendente o su designado; (2) toda grabación realizada bajo esta Orden podrá ser utilizada para evaluar la conducta y desempeño de los Agentes de la Policía, investigaciones criminales y en procedimientos administrativos, judiciales o legislativos; (3) toda solicitud interna o externa para revisar o distribuir una grabación en particular, tendrá que ser aprobada por el Superintendente o su representante designado.

17. Los parámetros establecidos en esta Orden General presentaron a esta Comisión interrogantes fundamentales sobre las garantías necesarias para la protección de los derechos humanos, como los derechos de libertad de expresión, asociación e intimidad, así como teniendo en mente los riesgos de la selectividad en la vigilancia y sus consecuencias.

D. El uso de otra tecnología de información en la Policía de Puerto Rico para fines investigativos

1. En la Inspección Ocular al CRADIC se mencionó el uso de "License Plate Readers", tecnología que detecta los números de las tablillas de vehículos de motor para contrastar con bases de datos sobre vehículos hurtados. En el panorama se encuentran técnicas sofisticadas de análisis

de información, ya sea visual o de otra clase, como por ejemplo, tecnologías de análisis predictivo e inteligencia artificial.

2. Bajo la Orden General 100-123 del 25 de abril de 2018, el Negociado de Tecnología Informática de la Policía, dirigido por el Dr. Juan Carlos Rivera Hernández, tiene como responsabilidad principal la "planificación, organización, implantación y mantenimiento de los sistemas computadorizados de información y comunicaciones" de la Policía de Puerto Rico.
3. Entre las funciones del Director, está administrar "toda actividad relacionada a la adquisición de tecnologías requeridas por las Superintendencias incluyendo sus divisiones, secciones y unidades de trabajo en términos de sus necesidades operacionales y administrativas." Asimismo, "velará porque todo [Miembro del Negociado de la Policía de Puerto Rico] esté debidamente adiestrado sobre la utilización de los sistemas de información" y "[a]nalizará y someterá recomendaciones sobre las normas y procedimientos relacionados con los sistemas de tecnología y comunicaciones que se implanten".
4. La adquisición de costosos "drones" sin políticas, sin planificación, sin permisos, y sin adiestramiento denota falta de integración entre el Negociado de Tecnología Informática y otros componentes de la Policía.

VI. Derecho Aplicable

En la evaluación de las cuatro áreas de investigación antes tratadas (prácticas de monitoreo, recopilación de información privada, grabación de actividades públicas y el uso de otra tecnología de información), se entrecruzan varios sistemas de protección de derechos en nuestro ordenamiento. El marco legal relevante a esta investigación comprende una diversidad de aspectos que incluyen derecho constitucional, parámetros establecidos en instrumentos internacionales de derechos humanos, así como normas estatutarias y otras declaraciones de política pública pertinentes.

En general, consideraremos las siguientes tres cuestiones de derecho en aras de evaluar los hallazgos relevantes a esta investigación:

1. Debemos tomar en cuenta la necesidad de que todo sistema de vigilancia gubernamental esté enmarcado en un régimen de controles y parámetros claros que eviten el ejercicio arbitrario de poderes estatales. Ello, a la luz de la normativa constitucional aplicable así como el ordenamiento internacional para la protección de derechos humanos y tomando en cuenta la experiencia con el monitoreo y persecución política por parte de las agencias investigativas del país.

2. Luego, consideraremos lo relacionado con el derecho a la libertad de asociación y expresión, así como los riesgos de que la acción gubernamental disuada la expresión social y política (el llamado "chilling effect").

3. Finalmente, miraremos lo relacionado al derecho a la intimidad en su vertiente constitucional y estatutaria a la luz de retos impuestos por nuevas tecnologías.

Todas estas cuestiones están íntimamente relacionadas entre sí por lo que no pueden verse como problemas separados: el derecho a la intimidad y la libertad de asociarse libremente con otras personas son precondiciones necesarias para la expresión y la manifestación pública de creencias políticas. Como planteó el entonces Juez Asociado Negrón García, "[d]espués de todo, la intimidad está inexorablemente vinculada no sólo a la personalidad, sino a la libertad de expresión política, fundamento de una sociedad libre."[116]

A. La necesidad de mecanismos de control: Persecución Política, "Carpetas" y Derechos Humanos

La experiencia histórica en Puerto Rico con la nefasta práctica de confeccionar expedientes o "carpetas" de personas por razones políticas claramente matiza este

[116] Opinión de Conformidad Juez Asociado Negrón García, *Noriega v. Gobernador*, 122 D.P.R. 650, 695 (1988).

informe. Los querellantes así han enmarcado su petición antes esta Comisión y, de igual manera, con esta experiencia en mente es que hemos considerado este asunto.

Y no es para menos. "Para decenas de miles de personas el mandato constitucional contra la discriminación ilegal resultó ser letra muerta por varias décadas. La Carta de Derechos de la Constitución del Estado Libre Asociado no cumplió su función protectora. Una especie de *apartheid* condenó a una porción de la población a ser víctima de hostigamiento y vigilancia por expresar y promover, según fuera el caso, ideas disidentes. Algunas prácticas de inteligencia típicas de países totalitarios fueron implantadas de forma regular..."[117] Esta historia es parte indeleble de nuestra realidad presente. "Constituye una mancha en nuestra vida colectiva de Pueblo que difícilmente será borrada.... Se presta para persecuciones, cacerías de brujas y para acallar justos reclamos. Equivale a sustituir la ley por la fuerza; la democracia por el totalitarismo."[118]

La relevancia de esta experiencia es más patente hoy que nunca, a la luz de los adelantos tecnológicos contemporáneos. El informe presentado por esta Comisión de Derechos Civiles en 1989[119] describió de forma detallada cómo trabajaba la División de Inteligencia de la Policía de Puerto Rico y la cantidad de recursos que se utilizaban en la creación de expedientes donde registraban detalladamente las actividades políticas y cotidianas de decenas de miles de individuos que se consideraban involucrados en

---

[117] Ramón Bosque Pérez y José Javier Colón Morera, Las Carpetas: Persecución política y derechos Civiles en Puerto Rico, pág. xiii (1997).

[118] Opinión de Conformidad Juez Asociado Negrón García, *Noriega v. Gobernador*, 122 D.P.R. 650, 696-697 (1988).

[119] Comisión de Derechos Civiles, 1989-CDC-028, Informe sobre discrimen y persecución por razones políticas: La práctica gubernamental de mantener listas, ficheros y expedientes de ciudadanos por razón de su ideología política (1989).

actividades caracterizadas vagamente como "subversivas", a través de procesos significativamente costosos. Los agentes e informantes tenían que ir físicamente a lugares, obtener documentos y fotografías que debían ser reveladas para sumarse a millones de documentos que ocupaban archivos y oficinas en estructuras de concreto. Igualmente, la magnitud de los recursos analíticos requeridos para navegar a través de esos documentos presentaba retos reales. En aquel entonces la División de Inteligencia tenía una oficina central que operaba desde el Cuartel General de la Policía de Puerto Rico. Tenía además, seis oficinas o unidades regionales en Arecibo, Mayagüez, Ponce, Caguas, Humacao y Aguadilla. Las funciones de estas oficinas giraban alrededor de la creación y mantenimiento de las mencionadas carpetas. En ese tiempo ni siquiera existía un sistema para clasificar y organizar a los investigados en términos de prioridad o frecuencia de investigación, lo que la división hacía según sus nociones de cuáles eran los grupos más importantes en el momento.[120]

Aún con las limitaciones prácticas que imponía la tecnología disponible en ese tiempo, el efecto de esta práctica fue desgarrador. Basta con destacar uno de los testimonios ofrecidos por uno de los miles de carpeteados por razones ideológicas. Juan Bautista Pérez, en ocasión de presentar su testimonio ante la Comisión de Derechos Civiles de Puerto Rico, manifestó que sin haber cometido delito alguno, sufrió un arresto ilegal en el 1950 por parte de un operativo de policías y guardias nacionales. Estuvo apresado nueve días en total, sin que se le acusara de delito alguno. Según

[120] Comisión de Derechos Civiles, 1989-CDC-028, Informe sobre discrimen y persecución por razones políticas: La práctica gubernamental de mantener listas, ficheros y expedientes de ciudadanos por razón de su ideología política (1989). Págs. 119-127.

Bautista, una vez le liberaron solicitó los expedientes tomados a su persona, mas no recibió respuesta de la agencia. Una vez comenzó a solicitar trabajo en distintos lugares, recibía contestaciones de que "era subversivo". Si lograba conseguir un trabajo, pocos meses después le despedían, pues los patronos recibían la vista del FBI, indisponiendo a sus patronos en su contra.

> Tuve que dedicarme a vender chucherías para sostener mis cinco hijos, quienes tuvieron que conformarse con escuela elemental, ya que yo no tenía recursos económicos...En 48 años no he tenido un solo día de tranquilidad por haber pertenecido a una lista de subversivos preparada por la Policía de Puerto Rico en violación a mis derechos como ciudadano.[121]

Hoy día, sin embargo, los métodos tecnológicos disponibles para llevar a cabo *dataveillance* y *dataprofiling*, para realizar vigilancia, recoger información de la conducta de personas en internet, y para almacenar esta información de las personas, hacen de los mecanismos de vigilancia contemporáneos exponencialmente más eficientes y, sin controles adecuados, aun más problemáticos.[122] Esta preocupación se hace evidente cuando consideramos "(1) [que la] internet hace posible agregar información personal proveniente de fuentes dispersas; (2) que la mayor parte de la información sobre nuestras prácticas cotidianas ya se encuentra disponible en formato digital y está lista para ser tomada; (3) la existencia de métodos de almacenamiento masivos relativamente económicos; y (4) la disponibilidad de computadoras potentes

[121] Comisión de Derechos Civiles, 1989-CDC-028, Informe sobre discrimen y persecución por razones políticas: La práctica gubernamental de mantener listas, ficheros y expedientes de ciudadanos por razón de su ideología política (1989). Págs. 52-53.
[122] Véase Barry Friedman, Unwarranted: Policing Without Permission (2017).

con capacidad de procesar la información con agilidad y generar perfiles individuales (sea para mercadeo o para el análisis de riesgos)".[123]

Es un hecho básico que la vigilancia genera información que debe almacenarse en bases de datos. Ese almacenamiento genera quizás una de las más complicadas controversias respecto al tema. Una vez fuera de nuestras manos, dicha información puede clasificarse, catalogarse y utilizarse de forma indiscriminada. La utilización de la internet y las redes sociales ha provocado prácticamente que dejemos un récord permanente de nuestras vidas, distribuido y esparcido por todas partes, listo para ser recopilado y catalogado por aquellos con la tecnología necesaria y por quienes tengan suficientes incentivos para hacerlo. El problema, por tanto, no es tanto la existencia de repositorios de información, videos u otra data, sino cómo se utiliza esta información, y qué controles reales existen que permitan evitar abusos.[124]

Mucha de la información personal en el entorno digital es recopilada por actores privados, en gran medida motivados por intereses comerciales y de mercadeo.[125] De otra parte, también los gobiernos recopilan información con el fin legítimo de proveer seguridad pública aunque, como se demostró en la época posterior a los ataques a las torres gemelas el 11 de septiembre de 2001, el interés en nuestra seguridad tiende a condicionar a la población a la noción de que es necesario sacrificar nuestras libertades.

Particularmente en tiempos de crisis, cuando nuestro sentido de seguridad pública es frágil y quebradizo, se asienta la idea de que debemos sacrificar algo de

---

[123] Hiram Meléndez Juarbe, La Constitución en Ceros y Unos: Un Acercamiento Digital al Derecho a la Intimidad y la Seguridad Pública,77 Rev. Jur. UPR 45 (2008), pág. 59. Sobre los retos que imponen nuevas tecnologías al derecho, véase, LAWRENCE LESSIG, CODE 2.0 (2006).
[124] The Digital Person, David Solove en la página 43.
[125] TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS (2016)

nuestros derechos mientras recibimos de forma acrítica cualquier tecnología que nos prometa seguridad y paz. Por eso, en muchos casos se presume sin cuestionamiento que los intereses de seguridad pública y los derechos humanos se encuentran en un estado de tensión permanente.[126] Aunque tal vez ese sea el caso en algunas circunstancias, la realidad es que adelantar la seguridad pública, aún en los momentos más difíciles, no siempre requerirá que entreguemos nuestras libertades.

En fin, la tecnología contemporánea es increíblemente eficiente y tiene la capacidad de superar muchos de los obstáculos físicos y prácticos que dificultaban obtener información en otros momentos. Esas ineficiencias tenían la consecuencia no anticipada de proveer una protección de facto al derecho a la intimidad y libertad de asociación, aún en los momentos más oscuros y tenebrosos en la historia de la persecución política del país. En la medida en que esas ineficiencias se superan por la agilidad tecnológica, desaparecen algunas de estas protecciones prácticas a nuestras libertades. Por tanto, en este contexto digitalizado, se hacen más necesarios que nunca sistemas rigurosos de control y mecanismos de vigilancia al que vigila.

Sobre la necesidad de mecanismos de control ante la recopilación de información el Tribunal Supremo de Puerto Rico, en *Vega v. Telefónica,* 156 D.P.R. 584 (2002), estableció parámetros que deben establecerse ante un sistema de vigilancia por cámaras de video. Si bien lo resuelto en ese caso fue en el contexto del empleo privado (tomando en cuenta que en Puerto Rico el derecho constitucional a la intimidad

[126] Hiram Meléndez Juarbe, La Constitución en Ceros y Unos: Un Acercamiento Digital al Derecho a la Intimidad y la Seguridad Pública,77 Rev. Jur. UPR 45 (2008).

aplica a las relaciones privadas),[127] los principios que emanan de ese dictamen son aplicables con más fuerza a la vigilancia gubernamental. Después de todo, las agencias gubernamentales con roles de vigilancia, como actores estatales, vienen principalmente llamadas a proteger los derechos constitucionales y son limitadas por estos derechos toda vez que ostentan el monopolio del uso legítimo de la fuerza.

En *Vega v. Telefónica* el Tribunal puntualizó la deseabilidad de reglamentación sobre el uso y disposición del material grabado, así como la necesidad de notificación adecuada a las personas sobre este sistema de video, y procedimientos para impugnar acciones del patrono basada en este material, entre otras cosas. Por ello, un sistema de vigilancia por cámaras, resolvió, debe evaluarse a partir de un análisis de factores que tome en cuenta tanto el interés en la seguridad y, de otro lado, el interés en proteger la intimidad y dignidad de las personas bajo vigilancia:

> [S]erá necesario analizar las circunstancias de cada situación o sistema de vigilancia en particular para determinar si éste constituye, ya sea por su naturaleza, o en su aplicación, una intromisión abusiva en la intimidad del empleado, o una violación a su dignidad e integridad. Cualquier evaluación a esos efectos debe comenzar con un análisis de las razones invocadas por el patrono para instalar el sistema, como por ejemplo: (a) seguridad, (b) reducir o prevenir incidencia de sabotaje o robos, (c) evaluar la efectividad o nivel de productividad del empleado, o (d) evaluar el trato que se le da al consumidor o cliente en el negocio. Luego de este análisis inicial, se podrá evaluar (1) cuán intrusivo es el método escogido por el patrono en la intimidad del empleado *vis a vis* el propósito y necesidad de la vigilancia; (2) las características particulares del lugar de empleo, como por ejemplo, si es un espacio abierto o cerrado, y la facilidad de acceso al mismo; (3) las funciones de los empleados observados; (4) la función de las facilidades que son objeto de vigilancia; (5) las capacidades técnicas y de sofisticación del equipo instalado; y (6) la publicación, notificación y utilización que haga el patrono del sistema, entre otras.

[127] *Arroyo v. Rattan Specialties*, 117 D.P.R. 35 (1986).

> En el contexto específico de la grabación en vídeo de determinada área de trabajo, debe considerarse: el campo de visión de las cámaras, su capacidad de hacer acercamientos o enfoques, periodos de tiempo que se encuentran encendidas, si las imágenes se graban o no, el periodo de tiempo durante el cual éstas se conservan, el acceso a las mismas y el uso que se les da, quién asume la responsabilidad por la conservación, control de acceso y disposición del material grabado, la política de la empresa a estos efectos, y la información que se le provea a los empleados sobre el sistema, entre otros.[128]

En cuanto al imperativo de que todo sistema de vigilancia por cámaras de video provea suficientes elementos de **notificación** a las personas que son objeto de las grabaciones, el Tribunal sentenció:

> [E]n aras de proteger la dignidad del trabajador, un patrono no debe establecer un sistema de vigilancia electrónica sin darle previa notificación a los empleados de la implantación del mismo, excepto en casos en que circunstancias apremiantes lo requieran. La notificación a estos efectos podría incluir, entre otras cosas, información sobre: (a) el tipo de vigilancia a utilizarse; (b) la naturaleza de los datos a obtenerse; (c) la frecuencia con que habrá de usarse el medio de vigilancia; (d) sus especificaciones técnicas; (e) lugar donde se instalará el sistema de vigilancia; (f) localización del equipo de monitoreo; (g) el grupo de empleados que ha de ser observado; y (h) el mecanismo administrativo disponible para canalizar las quejas de los empleados sobre el particular. Además, la empresa deberá tener una política clara y adecuada sobre el uso, disposición y acceso a la información recopilada, la cual se le informará a los empleados. Por último, como regla general, no se deberá instalar un sistema de videograbación de empleados en áreas en las cuales por su naturaleza, el empleado tenga una marcada expectativa de intimidad tales como los baños, duchas y vestidores (*locker rooms*).[129]

Asimismo, el Tribunal planteó la necesidad de que una entidad privada tenga un **reglamento que establezca parámetros claros** para el uso de los videos grabados, como mecanismo de controlar el uso arbitrario e indiscriminado del material, so pena

---

[128] *Vega v. Telefónica*, 156 D.P.R. 584, 608-609 (2002).
[129] Id. Págs. 611-612.

de que se restrinja la facultad que tiene el patrono para utilizar lo captado en video. Así, explicó:

> [L]a falta de reglamentación sobre el uso y disposición del material grabado, y la ausencia de un procedimiento para impugnar o explicar la conducta particular de un empleado ... que pueda ser captada por las cámaras, es un impedimento para que la PRTC pueda utilizar el material grabado para otros fines no relacionados con la seguridad en el [empleo]. La información recopilada por este sistema no deberá usarse indiscriminadamente, ni para cualquier propósito imaginable. En las circunstancias de este caso, la información obtenida deberá utilizarse para propósitos de proteger el equipo, la información y el propio personal del [empleo]. Así pues, no deberá usarse esta información como un método para vigilar conducta de los empleados que no esté relacionada con dichos propósitos de seguridad, como por ejemplo, evaluar la productividad o eficiencia de éstos. La información recopilada por las cámaras tampoco debe ser usada como base para tomar algún tipo de represalia contra los empleados ... por [ ] conducta captada que no esté relacionada con las razones de seguridad .... De esta forma lograremos un adecuado balance de intereses entre los derechos [del patrono] y los derechos de los empleados....

Como se ha dicho, las preocupaciones del Tribunal Supremo en el contexto privado son necesariamente trasladables al contexto público y deben servir de guía al considerar los hechos ante esta Comisión, en términos de la necesidad de que la recopilación de información privada tenga suficientes parámetros que eviten el mal uso y abuso de esta información, particularmente ante las capacidades de la tecnología digital. Esta conclusión se sostiene, además, tras considerar los abordajes que se han dado al problema desde una perspectiva de derechos humanos a nivel internacional.

La libertad de expresión, la libertad de pensamiento, libertad de asociación, reunión y manifestación, así como la libertad de difusión son derechos humanos reconocidos internacionalmente, tanto por la Organización de las Naciones Unidas como la Comisión Internacional de Derechos Humanos (CIDH). La Declaración

Universal de los Derechos Humanos, adoptada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948, dispone en su Artículo 18 que "[t]oda persona tiene derecho a la libertad de pensamiento, de consciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia."

De igual forma, el Artículo 19 del mencionado documento dispone que "[t]odo individuo tiene derecho a la libertad de opinión y de expresión". Según la Declaración, este derecho "incluye el no ser molestado a causa de las opiniones que se tengan, el de investigar y recibir información y opiniones y el de difundirlas sin limitación de fronteras por cualquier medio de expresión". El Artículo 20 dispone que "[t]oda persona tiene derecho a la libertad de reunión y de asociación pacíficas" mientras que el Artículo 12 dispone que "[n]adie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

Por otro lado, la Declaración Americana de los Derechos y Deberes del Hombre dispone en su artículo IV, que "[t]oda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio".

Atemperándose a los tiempos y tomando en consideración cómo la presencia física de los individuos ya equipara su presencia en el espacio virtual, el Consejo de Derechos Humanos de las Naciones Unidas aprobó la Resolución 20/08 del 5 de julio

de 2012, sobre la "Promoción, protección y disfrute de los derechos humanos en Internet" la cual dispone que todos los derechos que tienen las personas físicas deben ser protegidos en el ámbito digital. Así, contempla que el principio de libertad de expresión no se debe aplicar únicamente a los medios tradicionales sino también a la internet y todos los tipos de plataformas comunicativas de nuevo cuño.[130] Como recientemente sentenció el Tribunal Supremo de Estados Unidos en *Packingham v. North Carolina,* "[w]hile in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace—the "vast democratic forums of the Internet" in general, and social media in particular."[131]

De igual forma, el 18 de diciembre del 2013, la Asamblea General de las Naciones Unidas adoptó la Resolución 68/167[132] en la que expresó su preocupación sobre el efecto negativo que pueda tener la vigilancia y la interceptación de las comunicaciones, sobre los derechos humanos. De acuerdo a la resolución, la Asamblea General exhortó a los estados a que (1) respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales; (2) adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos; (3) examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la

[130] A/HRC/RES/20/8, https://digitallibrary.un.org/record/731540/files/A_HRC_RES_20_8-ES.pdf
[131] *Packingham v. North Carolina*, No. 15-1194, 582 U. S. ____ (2017).
[132] A/RES/68/167, https://undocs.org/es/A/RES/68/167

interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas las obligaciones en virtud del derecho internacional de los derechos humanos; (4) establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado.

A través de la resolución antes mencionada se encomendó la preparación del informe sobre el derecho a la privacidad en la era digital, el cual se produjo por la Oficina de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos.[133]. Este documento se enfoca en las prácticas de vigilancia masiva de distintos gobiernos a nivel internacional y enfatiza retos que presenta el ejercicio de derechos humanos en Internet. El informe concluye que la vigilancia invasiva, así como la recolección y el almacenamiento de datos personales derivados de la comunicación digital no solo puede infringir el derecho a la privacidad, sino también otros derechos fundamentales.

Entre los asuntos más importantes discutidos en este documento se encuentra la necesidad de *controles* expresados de forma transparente y accesible que limiten la arbitrariedad de las agencias estatales de vigilancia. Por ello, ningún estado debe adoptar leyes de vigilancia sin que haya normas o leyes que definan sus límites. Recalca dicho informe que:

---

[133] The Right to Privacy in the Digital Age, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

> The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse.[134]

Lo anterior fue determinado por la Alta Comisionada tomando en cuenta múltiples deficiencias encontradas en estos parámetros a nivel nacional:

> Practices in many States have... revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.[135]

El informe indica además que la ley o norma debe ser lo suficientemente accesible, clara y precisa, de manera que un individuo pueda buscarla y consultar quien está autorizado para recopilar información de vigilancia y bajo qué circunstancias. Debe probarse además que la limitación es necesaria para alcanzar un fin determinado y que esta sea la opción menos intrusiva. Finalmente, cualquier limitación al derecho de privacidad debe ser consistente con los otros derechos humanos, incluyendo la prohibición al discrimen. Cuando no se cumpla con estos criterios, la limitación será ilegal o la interferencia con el derecho a la intimidad será arbitrario.[136]

---

[134] Human Rights Council, The Right to Privacy in the Digital Age, A/HRC/27/37 (2014), disponible en http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf. Párrafo 28.
[135] Id. Párrafo 47.
[136] Id. Párrafo 23.

Otro elemento considerado por el sistema internacional de derechos humanos es la importancia de que las personas tengan información sobre las prácticas de recopilación personal, así como mecanismos para conocer la finalidad que se le da a la información y la posterior disposición de esta.[137] A tales efectos, el Comité de Derechos Humanos de las Naciones Unidas sostuvo que:

> [p]ara que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación.[138]

La *American Civil Liberties Union* y la organización *Human Rights Watch*[139] han alertado sobre la violación de derechos fundamentales que se lleva a cabo a través de programas de vigilancia masiva. En su reporte conjunto "*With Liberty to Monitor All: How Large-Scale Surveillance is Harming Journalism, Law and American Democracy*" estas organizaciones subrayaron la ausencia de transparencia, de mecanismos de rendición de cuentas y falta de conocimiento sobre cómo se dispone de

---

[137] Véase en general el General Data Protection Regulation, (EU) 2016/679.

[138] Naciones Unidas, Instrumentos Internaciones de Derechos Humanos. Volumen I: Recopilación de las Observaciones Generales y Recomendaciones Generales adoptadas por órganos creados en virtud de tratados de derechos humanos. HRI/GEN/1/Rev.9 (Vol.I). 27 de mayo de 2008. Pág. 228. 32º período de sesiones (1988). Observación general Nº 16. Derecho a la intimidad (artículo 17). Párr. 10. Disponible en https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=HRI/GEN/1/Rev.9%20%28Vol.%201%29&Lang=en

[139] With Liberty to Monitor All (2014), disponible en https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and

la información, de modo que se consagra una violación a los derechos humanos de las personas y un riesgo al sistema democrático de Estados Unidos en particular.

Por todo lo anterior, con el apoyo de lo que constituye un evidente consenso a nivel internacional, esta Comisión afirma que es indispensable el desarrollo de parámetros que controlen la discreción de los programas estatales de vigilancia. Independientemente de que podamos catalogar una situación particular como visible ante terceros o sobre la cual no hay una expectativa razonable de intimidad porque ocurre a la vista de todas y todos, es indispensable evitar el mal uso y abuso de estas facultades a toda costa. Por ello, resultan importantes las expresiones del entonces Juez Asociado Negrón García y que sirven de epígrafe a este informe:

> Sin controles, la labor investigativa gubernamental necesaria es dañina. Tiene el peligroso potencial de transformarse e institucionalizarse en espionaje oficial, capaz de sofocar el respetable derecho al pensamiento honrado, aunque éste signifique una postura de radical desavenencia ideológica frente al Estado y las mayorías. Incide en el derecho a la disidencia, materia prima natural e insustituible que abona las raíces del árbol de la democracia.[140]

La Comisión de Derechos Civiles de Puerto Rico afirma y adopta una serie de principios que deben guiar a todo forjador de política pública en esta área y que en particular deben influenciar el diseño de políticas y prácticas en la Policía de Puerto Rico. Se trata de principios elaborados por un amplia gama de organizaciones y de expertos en las áreas de privacidad y tecnología, con la ayuda de organizaciones como *Access, Privacy International* y la *Electronic Frontier Foundation*, con la participación del Sr. Frank La Rue, Relator Especial de las Naciones Unidas sobre la promoción y

[140] *Noriega v. Gobernador*, 122 D.P.R. 650, 698 (1988).

protección del derecho a la Libertad de opinión y de expresión.[141] El documento conocido como los "13 Principios Necesarios y Proporcionados" [142] ha sido firmado por más de 600 organizaciones que promueven y defienden los derechos humanos alrededor del mundo. Entre las organizaciones firmantes, en Puerto Rico están la Clínica de Nuevas Tecnologías, Propiedad Intelectual y Sociedad de la Escuela de Derecho de la Universidad de Puerto Rico y esta Comisión de Derechos Civiles.

Según el documento, cualquier programa de vigilancia electrónica desarrollada por un estado debe contener los siguientes principios:

> **Principio 1- Legalidad**
> Cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Dado el ritmo de los cambios tecnológicos, las leyes que limitan el derecho a la privacidad deben ser objeto de revisión periódica por medio de un proceso legislativo o reglamentario de carácter participativo.
>
> **Principio 2- Objetivo Legítimo**
> Las leyes sólo deberían permitir la vigilancia de las comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

---

[141] Véase, Electronic Frontier Foundation, Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance, https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf, nota al calce 1; Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 de abril de 2013, https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, Párrafo 10.

[142] Disponible en https://necessaryandproportionate.org.

Principio 3- Necesidad
Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La vigilancia de las comunicaciones sólo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.

Principio 4- Idoneidad
Cualquier caso de vigilancia de las comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.

Principio 5- Proporcionalidad
La Vigilancia de las Comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la vigilancia de las comunicaciones deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia.

Esto requiere que un Estado, como mínimo, debe demostrar lo siguiente—a una autoridad judicial competente—antes de la realización de la Vigilancia de las Comunicaciones para los fines de hacer cumplir la ley, la protección de la seguridad nacional, o la recolección de inteligencia:

1. Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo, y;
2. Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la Información Protegida, y;
3. Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica. y;
4. La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza especifica al fin legitimo alegado; y
5. Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud; y

6. La información será accesada solo por la autoridad especifica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización; y
7. Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

Principio 6- Autoridad Judicial Competente

Las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. La autoridad debe:

1. Estar separada e independiente de las autoridades encargadas de la vigilancia de las comunicaciones.
2. Estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la vigilancia de las comunicaciones, las tecnologías utilizadas y los derechos humanos, y
3. Tener los recursos adecuados en el ejercicio de las funciones que se le asignen.

Principio 7- Debido Proceso

El debido proceso exige que los Estados respeten y garanticen los derechos humanos de las personas asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general. Específicamente, al decidir sobre sus derechos, toda persona tiene derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley, salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos, debe buscarse una autorización con efecto retroactivo dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo.

Principio 8- Notificación del Usuario

Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados de la decisión de autorizar la vigilancia de comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación solo se justifica en las siguientes circunstancias:

1. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana; y
2. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia; y
3. El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.
4. La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones debe tener la libertad de notificar a las personas de la Vigilancia de las Comunicaciones, de forma voluntaria o bajo petición.

Principio 9- Transparencia

Los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades. Deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos. Los Estados deben proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la Vigilancia de las Comunicaciones. Los Estados no deberían interferir con los proveedores de servicios en sus esfuerzos para publicar los procedimientos que aplican en la evaluación y el cumplimiento de solicitudes de los Estados para la Vigilancia de Comunicaciones, se adhieran a esos procedimientos, y publicar los registros de las solicitudes de los Estados para la Vigilancia de las Comunicaciones.

Principio 10- Supervisión Pública

Los estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones.

Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, según proceda, al acceso a información secreta o clasificada para valorar si el Estado está haciendo un uso legítimo de sus funciones legales, para evaluar si el Estado ha publicado de forma transparente y precisa información sobre el uso y alcance de las técnicas y poderes de la vigilancia de las comunicaciones; y para formular determinaciones públicas en cuanto a la legalidad de dichas acciones,

incluyendo la medida en que cumplan con estos principios. Mecanismos de supervisión independientes deben establecerse, además de cualquier supervisión ya proporcionada a través de otra rama del gobierno.

Principio 11- Integridad de las Comunicaciones y Sistemas

A fin de garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que poner en peligro la seguridad con fines estatales casi siempre afecta la seguridad en términos generales, los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado. La retención o la recopilación de datos a priori nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anónimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios.

Principio 12- Garantías para la Cooperación Internacional

En respuesta a los cambios en los flujos de información y en las tecnologías y servicios de comunicaciones, los Estados pueden necesitar procurar la asistencia de un proveedor de servicios extranjero y otros Estados. En consecuencia, los tratados de asistencia judicial recíproca (MLAT, por sus siglas en inglés) y otros acuerdos celebrados por los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte la estándar disponible con el mayor nivel de protección para las personas. El principio de la doble incriminación debe ser aplicado en el momento en que los Estados procuren asistencia para efectos de hacer cumplir su legislación interna. Los Estados no pueden utilizar los procesos de asistencia judicial recíproca y las solicitudes extranjeras de Información Protegida para burlar las restricciones del derecho interno relativas a la Vigilancia de las Comunicaciones. Los procesos de asistencia judicial recíproca y otros acuerdos deben estar claramente documentados, a disposición del público y sujetos a las garantías de equidad procesal.

Principio 13- Garantías Contra el Acceso Ilegítimo y Derecho a Recurso Efectivo

Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los "whistle blowers" y medios de reparación a las personas afectadas. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba

> derivada de dicha información. Los Estados también deben promulgar leyes que establezcan que, después de que el material obtenido a través de la Vigilancia de las Comunicaciones ha sido utilizado con la finalidad por el que fue obtenida la información, el material no debe ser retenido, en su lugar, debe ser destruido o devuelto a los afectados.

B. La Libertad de Asociación, el derecho al anonimato y el efecto de la vigilancia en la auto inhibición expresiva (o "chilling effect")

El derecho a la intimidad no es un derecho unidimensional: no solo tiene que ver con el control sobre la información, sino también con nuestra capacidad de expresarnos y de formar relaciones sociales.[143] En este sentido, la intimidad interactúa con varios principios constitucionales: la libertad de expresión; el derecho a sostener relaciones íntimas; la democracia y los procesos deliberativos; la libertad de asociación y el anonimato.[144]

Tomemos como punto de partida la relación entre el derecho a la intimidad y la democracia. Charles Raab puntualiza de la siguiente forma el valor de la intimidad en nuestro sistema democrático y su importancia para la participación ciudadana:

> [L]a democracia participativa enfatiza la capacidad de actuar políticamente a través de la libertad de escoger, incluyendo las elecciones libres. No puede haber una libre elección en ausencia de la libertad de expresión, de organización y de reunión. El punto crucial es que estas libertades participativas requieren un grado de intimidad para su ejercicio; esto queda enfatizado por la relación entre las elecciones libres y el voto secreto, lo que promueve las decisiones políticas no coaccionadas.[145]

---

[143] Judith Wagner DeCew, In Pursuit of Privacy: Law Ethics and the Rise of Technology 73 (1997).
[144] Para una discusión sobre la multidimensionalidad del derecho a la intimidad, véase, Hiram Meléndez Juarbe, Privacy in Puerto Rico and the Madman's Plight: Decisions, 9 Georgetown J. Gen. & L. 1 (2008).
[145] Charles D. Raab, Privacy, Democracy, Information, en Brian D. Loader, Ed., The Governance of Cyberspace 155, 159-60 (1997).

En este sentido, existe una intersección entre la intimidad y la libertad de asociación que constituye eje esencial para la protección de la democracia. En la medida en que las asociaciones íntimas nos permiten excluir al gobierno de nuestras discusiones privadas y de la deliberación personal de nuestros puntos de vista, el derecho a la intimidad, fomenta la democracia. Así lo planteó un comentarista:

> Si una sociedad democrática requiere un proceso de deliberación vigoroso, el derecho a la intimidad es una precondición a la democracia en cuanto nos proporciona el espacio para considerar las controversias y formar opiniones antes de expresarlas a otros. En este sentido, la facultad de controlar lo que otros conocen sobre nosotros (controlar a quien revelamos lo que pensamos, nuestras ideas y nuestros calores) nos da la oportunidad de entrar en asociaciones íntimas solamente con aquellas personas con quien escojamos compartir nuestras preocupaciones sin temor a represalias por parte del gobierno o de nuestros pares.[146]

Así también lo ha reconocido el Tribunal Supremo de Estados Unidos al expresar la importancia de la asociación en agrupaciones políticas para nuestro sistema político, cuando afirmó que la defensa eficaz de puntos de vista diversos, especialmente los controversiales, requiere que se protejan proteger a asociaciones grupales de intromisión estatal indebida. Por esto, obligar a una agrupación proveer un listado de membresía constituiría una restricción de la libertad de asociación de sus miembros. [147]

La intersección entre intimidad y libertad de asociación es importante no solo en el contexto amplio de la democracia, sino también en el ámbito más personal del desarrollo individual. Así el derecho a la intimidad funge como mecanismo para que las personas puedan forjar relaciones significativas con otros y formar asociaciones.

---

[146] Hiram Meléndez Juarbe, La Constitución en Ceros y Unos: Un Acercamiento Digital al Derecho a la Intimidad y la Seguridad Pública,77 Rev. Jur. UPR 45 (2008).
[147] *N.A.A.C.P v. Alabama,* 357 U.S. 449 (1958).

Esto es esencial, ya que según discute Karst, la asociación con otros tiene una repercusión en la formación propia y en la manera forma en que un individuo moldea su identidad propia.[148] Esto es así ya que, a través de nuestras relaciones íntimas y de las asociaciones que formamos o integramos, delimitamos y controlamos la esfera de influencia que terceros y el Estado pueden tener sobre nuestro proceso de formación personal. La protección al valor constitucional de libertad de asociación reconoce que los individuos obtienen mucho de su enriquecimiento personal de los lazos que se forman con otros. En la medida en que las asociaciones íntimas nos permiten excluir al gobierno de las discusiones privadas y la deliberación personal de nuestros puntos de vista, se salvaguarda un valor esencial de la convivencia social.[149]

El Tribunal Supremo de Estados Unidos validó puntualmente esta característica del derecho a la asociación en el caso *Roberts v. United States Jaycees*, donde definió los contornos del derecho a la asociación. Según una autora, esta jurisprudencia reconoce que:

> el derecho a la libre asociación se divide en dos vertientes: la asociación expresiva y la asociación íntima. En la primera vertiente, la libertad de asociación se protege por ser necesaria para practicar aquellos derechos garantizados por la Primera Enmienda, como la libertad de expresión o de practicar una religión. El derecho a la asociación íntima, por su parte, preserva la libertad de mantener ciertas relaciones íntimas frente a las intromisiones indebidas del Estado. Esta vertiente del derecho a la asociación constituye, por tanto, un elemento de la libertad personal. De esta definición del derecho a la asociación íntima puede verse la identidad entre el derecho a la intimidad y el derecho a la asociación cuando se trata de una situación en la que se busca salvaguardar la

[148] Kenneth L. Karst, The Freedom of Intimate Association, 89 YALE L. J. 624, 635-36 (1980).
[149] Hiram Meléndez Juarbe, Privacy in Puerto Rico and the Madman's Plight: Decisions, 9 Georgetown J. Gen. & L. 1 (2008).

> autonomía de las personas de decidir en qué relaciones quieren entrar y de mantener la información sobre esas relaciones confidenciales.[150]

Otro valor fundamental para la democracia y la libertad de expresión es el anonimato. El llamado *discurso anónimo* implica de por sí una participación en el debate público, en la que por alguna razón específica el emisor o la emisora no revela su identidad. Según Alan Westin "el anonimato ocurre cuando el individuo se encuentra en lugares públicos o realiza actos públicos pero aún busca y encuentra libertad de ser identificado o vigilado.... El conocimiento o el miedo de que se esté siendo observado sistemáticamente en lugares públicos destruye el sentimiento de tranquilidad y libertad que las personas buscan en espacios abiertos".[151] Por esta razón, el derecho a permanecer anónimo es una dimensión externa o expresiva de ese derecho a la intimidad, cuando se vincula con otros valores constitucionales a protegerse.

Sobre la importancia del anonimato, la Relatoría Especial de la Organización de Naciones Unidas sobre Promoción y Protección del Derecho a la Libertad de Protección discutió en su informe del 2013 el vínculo entre la intimidad y el anonimato como garante de la protección a la libertad de expresión y como elemento importante para la movilización social mediante la protesta pública.

> Tanto el derecho a la libertad de pensamiento y expresión como el derecho a la vida privada protegen el discurso anónimo frente a restricciones estatales. La participación del debate público sin revelar la identidad del emisor es una práctica usual en las democracias modernas. La protección del discurso anónimo favorece la participación de las personas en el debate público ya que – al no revelar su identidad— pueden evitar ser objeto de represalias injustas por el ejercicio de un

[150] María D. Trelles Hernández, Silencio en la Corte: La Aplicación e Implicaciones del Derecho a la Intimidad en las Agencias de Ley y Orden Público, 72 Rev. Jur UPR 971, 979 (2003).
[151] ALAN WESTIN, PRIVACY AND FREEDOM 31 (1967) (traducción suplida).

> derecho fundamental. En efecto, quienes ejercen el derecho a la libertad de pensamiento y de expresión participan del debate público y de la vida política de una comunidad. Ello no supone –solamente—escribir notas de opinión o participar en foros de debate: también supone la posibilidad de llamar a movilizaciones sociales, de convocar a otros ciudadanos a manifestarse, de organizarse políticamente o de cuestionar a las autoridades, aún en situaciones de riesgo.[152]

Así lo ha ratificado el Tribunal Supremo de Estados Unidos, al reconocer que el permanecer en anonimato es un elemento esencial del ejercicio de los derechos de libertad de expresión y libertad de asociación, contenidos en la Primera Enmienda de la Constitución de Estados Unidos. En *Talley v. State of California*, 362 U.S. 60 (1960), el Tribunal Supremo determinó que una ordenanza municipal que prohibía la entrega de folletos, a menos que estos tuvieran el nombre y las direcciones de los autores o auspiciadores, violaba los derechos de expresión y prensa contenidos en la Primera Enmienda. Escribiendo para la mayoría el Juez Hugo Black resaltó el rol histórico del anonimato en las publicaciones, al destacar que solo a través del anonimato diversos grupos han podido criticar prácticas y leyes opresivas. A esos efectos, indicó lo siguiente:

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies, was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in

[152] CIDH (2013). Informe de la relatoría especial para la libertad de expresión. Capítulo IV (Libertad de expression e internet). OEA/Serv.L/V/II.149. Par. 134. Obtenido el 6 de febrero de 2015, de http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_IA_2013_ESP_FINAL_WEB.pdf.

> England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers.[153]

A igual conclusión llegó el tribunal en *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), cuando afirmó que el discurso anónimo está protegido por la Primera Enmienda y que dicha protección no solo abarca la producción literaria sino el activismo en torno a causas políticas. En el citado caso indicó:

> Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation –and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.

La relación entre el derecho a la intimidad, la libertad de asociación, la participación política en una democracia y el anonimato, demuestran una particularidad que es esencial para este informe. Al igual que en la discusión anterior sobre la necesidad de controles a la gestión de vigilancia del Estado, las preocupaciones detrás de la vigilancia gubernamental no giran alrededor de si el comportamiento en cuestión ocurre en público a la vista de otras personas. Es decir, los problemas con el anonimato y la libertad de asociación mediante mecanismos de vigilancia ubicua no se suscitan solamente cuando se penetra un velo de secretividad. Todo lo contrario: cuando los ciudadanos y las ciudadanas actúan en la esfera pública tienen razones legítimas para esperar que su anonimato sea preservado, como mecanismo para potenciar su libertad

[153] *Talley v. State of California*, 362 US 60, 64-65 (1960).

de asociación y su libertad de expresión. Cuando el derecho y la tecnología limitan nuestra habilidad de controlar nuestra identidad en público, la falta de anonimato puede producir un efecto disuasivo (el llamado "chilling effect"), perjudicial a la diversidad y riqueza del discurso. Así la democracia puede verse amenazada.

De acuerdo con Frederic Shauer *"[a] chilling effect occurs when individuals seeking to engage in activity protected by the first amendment are deterred from so doing by governmental regulation not specifically directed at that protected activity."*[154] Es decir, se trata de aquellas situaciones en una persona se inhibe de incurrir en conducta expresiva que está constitucionalmente protegida a causa de acción gubernamental. En palabras de Schauer:

> [E]l daño de esta clase de *chilling effect* en los individuos recae en el hecho de que algo que debería ser expresado no lo es. Disuadido por el miedo al castigo, algunos individuos se inhiben de decir o publicar aquello que podría, y de hecho debería, legalmente ser difundido. Esto debe ser temido no solo por el daño que surge del no ejercicio de un derecho constitucional, pero también por la pérdida social que resulta cuando las libertades garantizadas por la Primera Enmienda no son ejercidas.[155]

Una situación de vigilancia por medio de mecanismos tecnológicos (ya sea por redes sociales, por video u otros medios) crea una consciencia social de que los actos de los individuos pueden ser minuciosamente escrutados. Esta consciencia social sobre la vigilancia tiene un efecto pernicioso sobre el ejercicio de los derechos: "una vez la población se acostumbra a ser observada las veinticuatro horas del día y los siete días de la semana, el sentimiento panóptico se integra a la conciencia colectiva, se tatúa en

---

[154] Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 Boston University Law Review 685, 693 (1978).
[155] Id. Pág. 693.

la piel, y es aceptado."[156] La conducta pública de las personas (conducta protegida por los derechos de libertad de expresión), por tanto, se ve condicionada y afectada por el conocimiento de su vigilancia.

Todo lo anterior levanta serias preocupaciones sobre los hechos encontrados en este informe. Las manifestaciones de la entonces Superintendente de la Policía sobre el monitoreo en las redes sociales, unido a la cobertura mediática de estas expresiones apenas unos días antes de las manifestaciones del 1ro de mayo de 2017, revelan actos que—independientemente de su intención—muy probablemente tuvieron el efecto de crear un efecto disuasivo sobre el ejercicio de derechos constitucionales de personas que participaron (o que no participaron) de esas protestas. A ello se le suma la actividad coordinada de la Policía de Puerto Rico con el FBI al referirle comentarios de personas en Facebook unos días antes de la protesta, y el consiguiente procesamiento (judicial y en los medios) de una persona por sus expresiones en redes sociales. Todos estos actos, unidos a la presencia casi permanente de la Sección Técnica de Grabaciones en toda actividad de protesta pública en Puerto Rico tiene, indudablemente, un efecto en el ejercicio de derechos humanos en el país: afecta el sentido de anonimato de las personas

---

[156] Hiram Meléndez Juarbe, La Constitución en Ceros y Unos: Un Acercamiento Digital al Derecho a la Intimidad y la Seguridad Pública,77 Rev. Jur. UPR 45 (2008). Véanse además, REG WHITAKER, THE END OF PRIVACY 40-42 (1999); MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 184-185 (1977):

> The examination combines the techniques of an observing hierarchy and those of a normalizing judgment. It is a normalizing gaze, a surveillance that makes it possible to qualify, to classify and to punish. It establishes over individuals a visibility through which one differentiates them and judges them. That is why, in all the mechanisms of discipline, the examination is highly ritualized. In it are combined the ceremony of power and the form of the experiment, the deployment of force and the establishment of truth. At the heart of the procedure of discipline, it manifests the subjection of those who are perceived as objects and the objectification of those who are subjected. The superimposition of the power relations and knowledge regulations assumes in the examination all its visible brilliance.

en el espacio público, incide sobre la libertad de asociación, mina la confianza en la protección de derechos durante la planificación y ejecución de actividades de protesta y, en fin, socava presupuestos importantes de una democracia.

Sobre estas preocupaciones con el "chilling effect" de la vigilancia pública subrayamos algunos aspectos preocupantes de la dinámica antes mencionada entre la Policía de Puerto Rico y el FBI en momentos cercanos a la protesta. Como se destacó en la porción de hallazgos de este informe, existe en récord una serie de referidos de ciertas expresiones de personas en Facebook que fueron catalogadas por la Policía de Puerto Rico como "amenazas" y que, al menos en un caso, fueron encausadas criminalmente por la agencia federal. Por el efecto disuasivo que esta dinámica (especialmente dada su publicidad) puede tener sobre el ejercicio de derechos de protesta, es meritorio detenernos a considerar la legitimidad de estos actos. Toda vez que mucha de esta expresión es constitucionalmente protegida, aunque parezca indeseable, nos parece preocupante—y muy cuestionable—que se activen los mecanismos del Estado para estos fines.

La premisa del sistema de libertad de expresión aplicable en nuestra jurisdicción, es que las discusiones sobre asuntos de interés públicos en foros públicos deben protegerse sin intervención Estatal, aun cuando su forma y contenido sean odiosos y ofensivos, salvo en limitadas circunstancias. Así, por ejemplo, el Tribunal Supremo de Estados Unidos expuso en *Snyder v. Phelps*, 562 U.S. 443, 12 (2011), que:

> [S]peech at a public place on a matter of public concern, ... is entitled to "special protection" under the First Amendment. Such speech cannot be restricted simply because it is upsetting or arouses contempt. "If there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because

> society finds the idea itself offensive or disagreeable." Indeed, "the point of all speech protection . . . is to shield just those choices of content that in someone's eyes are misguided, or even hurtful."

Por esto, no toda expresión que parezca una amenaza puede castigarse o prohibirse. Solamente las llamadas "amenazas reales" (o "true threats" según el Tribunal Supremo de Estados Unidos) pueden restringirse de conformidad con la garantía a la libertad de expresión en la Primera Enmienda. Esto es así porque, aunque no es permitido que el Estado prohíba expresión pública sobre asuntos de interés público, *es legítimo evitar aquellas circunstancias que engendren temor en las personas.*[157]

Según el Tribunal Supremo en *Virginia v. Black*, 538 U.S. 343 (2003), la amenaza real es aquella en que una persona expresa una **intención seria de cometer un acto violento contra una persona o grupo de personas.**

> "True threats" encompass those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals. The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats "protect[s] individuals from the fear of violence" and "from the disruption that fear engenders," in addition to protecting people "from the possibility that the threatened violence will occur."[158]

La intimidación, por ejemplo, es una "especie de amenaza real, en que alguien dirige una amenaza a otra persona o a un grupo de personas con la intención de crear temor en la víctima de daño corporal o la muerte".[159] Por el riesgo de que se castigue la expresión protegida con el pretexto de limitar las amenazas reales, es importante que

---

[157] *Virginia v Black*, 538 U.S. 343 (2003).
[158] Id. Págs. 359-360 (2003).
[159] Id. Pág. 344.

todos los operadores estatales ejerzan sumo cuidado en su tratamiento de esta conducta: tanto la Rama Legislativa al codificar delitos pertinentes, como en la Rama Ejecutiva al encausarlos y la Rama Judicial al adjudicarlos.

Por lo anterior, el Tribunal Supremo de Estados Unidos ha sido muy claro en cuanto a que la "hipérbole política" (aunque parezca una amenaza) no puede catalogarse como una amenaza real y, por ende, castigarse. En *Watts v. United States*, 394 U.S. 705 (1969), ese Tribunal consideró una acusación a una persona que emitió lo que pareció una amenaza al Presidente de los Estados Unidos. El delito que en cuestión prohibía "knowingly and willfully [making] any threat to take the life of or to inflict bodily harm upon the President of the United States" 18 USC 871(a). En el contexto de una discusión pública en Washington, D.C., el acusado Watts se había expresado en contra del servicio militar obligatorio, y en el calor de la discusión manifestó el aparente deseo de dispararle al Presidente Lindon B. Johnson: "now I have already received my draft classification as 1-A and I have got to report for my physical this Monday coming. I am not going. **If they ever make me carry a rifle the first man I want to get in my sights is L.B.J...** They are not going to make me kill my black brothers."

Al considerar estas expresiones así como la prohibición estatutaria, el Tribunal indicó que es necesario interpretar el delito de amenazas "against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and

sometimes unpleasantly sharp attacks on government and public officials."[160] Al proteger lo que es una manifestación cruda de oposición al Presidente, el Tribunal reconoció que el lenguaje en la arena política es en ocasiones "vituperado, abusivo e inexacto", y así debe asumirse.[161]

Toda expresión debe tomarse en su contexto, claro está. Pero resulta evidente que muchas de las manifestaciones en redes sociales referidas al FBI por la Policía de Puerto Rico tienen características de hipérbole política o carecen de los elementos que constituyen una amenaza seria de acto violento. Así, por ejemplo, a todas luces constituye una manifestación política hiperbólica expresar en Facebook "[q]ue prendan en fuego el capitolio" o, expresar en Facebook durante las protestas del 1ro de mayo de 2017 "Eso es, que hagan lo que tengan que hacer, que exploten el capitolio si es necesario. Una revolución es lo que hace falta." Si bien el sentido violento de estas expresiones deja mucho que desear en torno al carácter del discurso público, también es cierto que ningún funcionario del gobierno puede activar la maquinaria punitiva Estatal como reacción a manifestaciones desagradables u ofensivas, a no ser que se trate de expresiones desprotegidas como las "amenazas reales" o cualquier otra categoría de expresión desfavorecida por la Constitución.[162]

Destacamos las manifestaciones de una persona que, más allá de referirse al FBI, fue en efecto encausada criminalmente. Como se relató en la porción de hallazgos de este informe, una persona fue arrestada y acusada luego de decir en Facebook

---

[160] *Watts v. United States*, 394 U.S. 705, 708 (1969).
[161] Id. 708.
[162] Véase, *Cohen v. California*, 403 U.S. 15 (1971).

"Vamos a bombardear el Capitolio y que en paz descansen nuestras conciencias". El delito cuya violación se imputó fue el de amenazas tipificado en 18 USC § 844(e).

Esta ley federal castiga a:

> Whoever, through the use of [an] instrument of interstate ... commerce ... **willfully makes any threat**, or maliciously conveys false information knowing the same to be false, concerning an attempt or alleged attempt being made, or to be made, to kill, injure, or intimidate any individual or unlawfully to damage or destroy any building, vehicle, or other real or personal property by means of fire or an explosive.

Nótese que el delito imputado tiene como elemento específico el que la persona exprese **intencionalmente una amenaza ("willfuly")**. En *Elonis v. United States*, No. 13-986, 575 U. S. ____ (2015), el Tribunal Supremo resolvió para otro delito federal de amenazas que guarda silencio en torno al nivel de intención,[163] que la persona acusada de amenazas debe tener algún grado de intención en cuanto a que la comunicación es amenazante. *Elonis, id.* ("The mental state requirement must...apply to the fact that the communication contains a threat"). Es decir, aun si el delito carece de un requisito de intención en el texto de la ley, emitir expresiones *negligentemente* es insuficiente, de modo que *no puede castigarse a una persona al amparo de un delito federal sólo porque sus expresiones puedan razonablemente interpretarse por otros como amenazantes*. En el caso del delito imputado por el FBI ante las expresiones aquí señaladas sobre "bombardear el Capitolio", se destaca que la referida ley sí requiere intención específica de amenazar ("willfully makes any threat") o al menos el

[163] El delito considerado en *Elonis* castiga a una persona que "transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another". 18 USC § 875(c).

conocimiento de que su expresión será percibida como una amenaza,[164] por lo cual era indispensable que se demostrara esa intención específica. Cabe reiterar que, eventualmente, los cargos contra el acusado fueron desestimados.

Es decir, como cuestión constitucional, no pueden castigarse expresiones que articulen una aparente amenaza cuando se trate de un argumento político cáustico y estridente, en lugar de una "amenaza real" (en otras palabras "[a] serious threat as distinguished from words as mere political argument, idle talk or jest")[165]. Además, como cuestión estatutaria es insuficiente que meramente la expresión pueda ser razonablemente interpretada como una amenaza, pues la intención amenazante del que se expresa es crucial.[166] **Es decir, no puede castigarse a una persona sólo por expresarse en redes sociales contra el gobierno o sus funcionarios cuando es una forma de expresión política, aun cuando se hace en términos agresivos**. Si algo resulta claro de nuestro sistema de libertad de expresión es que el Estado está impedido de filtrar el discurso público sobre asuntos de interés público, salvo que concurran circunstancias especiales.

Por otra parte, además de desarrollar la doctrina de las "amenazas reales", el Tribunal Supremo de los Estados Unidos ha establecido que un gobierno no puede coartar conducta expresiva, sólo por el hecho de que esta expresión incite a la violencia o a la violación de la ley. El Estado puede prohibir esta conducta en casos extremos en que la conducta esté específicamente dirigida a motivar la violación de la ley y

---

[164] El Tribunal Supremo en *Elonis* articuló lo que constituiría un requsito de intención específica de intimidar como "if the defendant transmits a communication for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat", *id.* pág 16.
[165] *United States v. Spruill*, 118 F.3d 221, 228 (4th Cir.1997).
[166] *Elonis*, *id.* pág. 14 ("what [Elonis] thinks' does matter").

únicamente cuando sea inminente (altamente probable) que eso va a ocurrir. Este es el fundamento central del caso *Brandenburg v. Ohio*:

> the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.[167]

Enfatizamos el alcance de este mandato constitucional. El Estado no puede prohibir conducta expresiva sólo porque piense que es posible que se va a violentar la ley. Solamente puede actuar en aquellos casos en que la conducta ilegal sea verdaderamente inminente o altamente probable que ocurrirá.

Las consideraciones anteriores se tornan cada vez más importantes cuando tomamos en cuenta la centralidad de las redes sociales para el discurso público contemporáneo, con sus ventajas y desventajas. Como planteó el Tribunal Supremo, no cabe duda cuál es el espacio más importante hoy día para el intercambio de ideas: "It is cyberspace—the 'vast democratic forums of the Internet' in general, and social media in particular."[168] Según explicó el Tribunal:

> Social media offers "relatively unlimited, low-cost capacity for communication of all kinds." On Facebook, for example, users can debate religion and politics with their friends and neighbors or share vacation photos. On LinkedIn, users can look for work, advertise for employees, or review tips on entrepreneurship. And on Twitter, users can petition their elected representatives and otherwise engage with them in a direct manner.[169]

---

[167] *Brandenburg v. Ohio*, 395 US 444, 447 (1969).
[168] *Packingham v. North Carolina*, No. 15-1194, 582 U. S. ____ (2017).
[169] Id. Pág. 8.

En este sentido, debemos dar cuenta de las dinámicas expresivas en internet y, particularmente, las normas de comportamiento forjadas en redes sociales. Así, por ejemplo, la expresión en redes sociales tiende a ser informal y desinhibida. Como articulan Lidsky y Norbut:

> People access Twitter, Facebook, and Instagram through phones or computers, and the technology psychologically distances them from the impact of their words, leading people to say things online that they would never say in person. The disinhibiting effect of the technology is increased further if the speaker also posts anonymously or pseudonymously. Even the speed of communication may foster incendiary speech: speakers respond to provocations before good sense can assert itself. And, of course, no editor stands between speaker and audience to interpose good judgment prior to publication.[170]

Como la discusión en redes sociales no ocurre ante la presencia física de los interlocutores, es particularmente susceptible de malinterpretarse. En este contexto puede ser muy fácil confundir, por un lado, expresiones estridentes y hasta groseras que operan en el terreno de la hipérbole constitucionalmente protegida con, de otro lado, amenazas reales que pueden prohibirse. Así, "[i]t is easy for 'outsiders,' including legal decision-makers, to misconstrue speech in social media. Such misconstructions may include interpreting violent hyperbole as true threats."[171]

Probablemente la mayoría de las personas que interactúan en redes sociales y expresan oposición al gobierno en términos que reflejan agresividad lo hacen bajo el manto de la protección constitucional y, además, siguiendo códigos informales de conducta social que resultan relativamente comunes en esos espacios. En estas

---

[170] Lyrissa Barnett Lidsky & Linda Riedemann Norbut, *#I[*]U: Considering the Context of Online Threats*, 106 Cal. L. Rev. 1885, 1910 (2018).
[171] Id. Pág. 1913.

circunstancias sería chocante para cibernautas, y retaría sus expectativas sobre lo que es comportamiento apropiado en las redes sociales, conocer que su conducta constitucionalmente protegida es referida a autoridades federales y, posiblemente, encausada criminalmente. Nada de esto implica que no existan "amenazas reales" en la internet—particularmente cuando la conducta amenazante se dirige a una persona o grupo de personas en particular, causando temor a su vida o seguridad, y se hace con la intención de provocar ese temor. Sabemos que existen y deben ser atendidas ágilmente, especialmente cuando estas amenazas reales constituyen (como en muchas ocasiones) patrones de hostigamiento y acoso por razón de género. Pero en el caso de expresión hiperbólica en redes sociales, de índole social y política, es muy posible que la acción estatal se active equivocadamente con la consecuencia de acallar manifestaciones políticas legítimas.

Por lo anterior, es particularmente arriesgado que el Estado active sus mecanismos punitivos en las zonas grises entre la expresión protegida y la desprotegida. El riesgo de provocar un efecto inhibidor o "chilling effect" es, en estos casos, intolerablemente alto. Además, el riesgo de crear un efecto inhibidor a la expresión protegida es aun mayor cuando, a días de una protesta masiva, los agentes de orden público federales alardean públicamente sobre el castigo a una persona que muy probablemente ejercía sus derechos constitucionales. Como mínimo, tomando en cuenta los riesgos de crear un efecto disuasivo en la expresión, este despliegue oportuno de fuerza y publicidad puede considerarse como imprudente.

C. *El Derecho a la Intimidad y el Derecho a Controlar la Información Privada Aún en Público*

En la Constitución de los Estados Unidos, el derecho a la intimidad no está explícitamente establecido. Fue a partir de un proceso histórico que el Tribunal Supremo reconoció, como parte del concepto de *libertad* de las cláusulas de Debido Proceso de Ley de su Constitución la existencia de tal derecho como uno de naturaleza fundamental.[172] Distinto a ese desarrollo, la Constitución de Puerto Rico reconoce explícitamente la existencia de este derecho en las secciones primera y octava del artículo II. Así, la sección 8 de nuestra Carta de Derechos dispone que "[t]oda persona tiene derecho a protección de ley contra ataques abusivos a su honra, a su reputación y a su vida privada o familiar", mientras que la sección 1 expresa que "La dignidad del ser humano es inviolable ".

El Informe de la Comisión de la Carta de Derechos de la Asamblea Constituyente de Puerto Rico enfatizó la importancia y amplitud de dicha sección 8 y señaló la relación entre ésta y la sección 1:

> La protección contra ataques a la honra, reputación y vida privada constituye también un principio que complementa el concepto de la dignidad humana mantenido en esta constitución. Se trata de la inviolabilidad personal en su forma más completa y amplia. El honor y la intimidad son valores del individuo que merecen protección cabal, no sólo frente a atentados provenientes de otros particulares, sino también contra ingerencias abusivas de las autoridades. . . .[173]

---

[172] Véanse *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Loving v. Virginia*, 388 U.S. 1 (1967); *Eisenstaat v. Baird*, 405 U.S. 438 (1972); *Roe v. Wade*, 410 U.S. 113 (1973).

[173] 4 DIARIO DE SESIONES DE LA CONVENCIÓN CONSTITUYENTE 2566.

Además, nuestro texto constitucional incluye una sección equivalente a la enmienda Cuarta de la Constitución Federal, ambas dirigidas a prohibir las detenciones, registros y allanamientos irrazonables. La enmienda Cuarta Federal establece que

> [t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized.[174]

La sección diez de nuestra Constitución establece por su parte que:

> No se violará el derecho del pueblo a la protección de sus personas, casas, papeles y efectos contra registros, incautaciones y allanamientos irrazonables.
>
> No se interceptará la comunicación telefónica.
>
> Sólo 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.[175]

Como se puede apreciar, nuestro texto constitucional tiene una equivalencia casi directa con el de la Constitución Federal al menos en cuanto a las cláusulas primera y tercera; existencia independiente tiene la cuarta cláusula (regla de exclusión) y; total originalidad tiene la segunda (prohibición de interceptación de comunicación telefónica).

---

[174] CONST. E.E.U.U. Enda. IVta.
[175] CONST. P.R. Art. II, § 10.

En el ámbito internacional, la intimidad también ha logrado reconocimiento. La Declaración Universal de los Derechos Humanos aprobada en el 1948, en su artículo 12 de consignó que ninguna persona debe ser "[o]bjeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación". Se dispuso también que toda persona tiene derecho a la protección de ley contra tales injerencias o ataques. Esta disposición fue adoptada en el Pacto Internacional de Derechos Civiles y Políticos de 1966, en su artículo 17.

Asimismo, el artículo 11 de la Convención Americana sobre Derechos Humanos dispone que "[t]oda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; y que "[n]adie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación". Finalmente, la Convención sobre los Derechos del Niño de 1989, en su artículo 16, establece que ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación. También establece que los niños deberán tener protección de tales ataques o interferencia.

Nuestro Tribunal Supremo en innumerables ocasiones ha reiterado la mayor amplitud del alcance de nuestra protección constitucional. Así, por ejemplo, en *E.L.A. v Hermandad de Empleados,*[176] el Tribunal Supremo señaló que la intención de los constituyentes, era "formular una Carta de Derechos de *factura más ancha* que la tradicional, que recogiese el sentir común de culturas diversas sobre nuevas categorías

[176] 104 D.P.R. 436 (1975).

de derechos. De ahí que la Declaración Universal de los Derechos del Hombre y la Declaración Americana de los Derechos y Deberes del Hombre ejerciesen una influencia tan significativa en la redacción de nuestra Carta de Derechos".[177] Por eso se ha dicho que "[n]uestra Constitución reconoce y concede unos derechos fundamentales con una visión más abarcadora y protectora que la Constitución de Estados Unidos".[178]

Asimismo, en *Cortés Portalatín v. Hau Colón*,[179] se enfatizó la amplitud de nuestro derecho a la intimidad al catalogarlo como

> un principio con aspiraciones de universalidad, destilado de muy diversos sistemas jurídicos, ancho es el mundo que se nos brinda para su interpretación justa. No se está obligado por juegos específicos de reglas históricas. La obligación es acatar el mandato constitucional, en consonancia con otras disposiciones de nuestra ley primaria y las realidades del país.

El Tribunal Supremo también ha sostenido que el derecho a la intimidad "impone a toda persona el deber de no inmiscuirse en la vida privada o familiar de los demás seres humanos".[180] De ahí que se entienda que este Derecho es inclusive oponible a personas particulares, no sólo ante el Estado, y que opera *ex propio vigore*, sin necesidad de ulterior acción legislativa.[181] Esta tradición de "factura más ancha" en el derecho a la intimidad, ha provocado cierta sensibilidad del Tribunal a los retos que los desarrollos tecnológicos imponen a la protección de los derechos constitucionales. Así, en *Arroyo v. Rattan Specialties*, el Tribunal expuso que:

> [d]ebemos sentar las pautas para el uso adecuado de los adelantos científicos y tecnológicos de forma tal que nos ayuden a confrontarnos

---

[177] Id. Pág. 440 (énfasis suplido).
[178] López Vives v. Policía de P.R., 118 D.P.R. 219, 226-27 (1987). *Véase además*, 3 JOSÉ TRÍAS MONGE, HISTORIA CONSTITUCIONAL DE PUERTO RICO 169-70 (1980).
[179] 103 D.P.R. 734, 738 (1975).
[180] *Colón v. Romero Barceló*, 112 D.P.R. 573, 576 (1982).
[181] *Arroyo v. Rattan Specialties*, 117 D.P.R. 35, 75 (1986).

> con los difíciles problemas de la sociedad moderna, sin que la ansiedad por soluciones fáciles y rápidas nos haga perder de vista la necesidad de proteger y preservar los valores más esenciales para el hombre. 'Debe recordarse que la ciencia y técnica vive una voluntad de poder no restringida por valoraciones que puede llevar a un despotismo más o menos fuerte de la vida social que esquematiza y uniforma sin tomar en cuenta lo individual, lo humano.'[182]

En el marco de lo anterior, uno de los lentes a través de los cuales los tribunales avalúan los límites a la acción investigativa estatal es la prohibición constitucional a *registros y allanamientos irrazonables* y su relacionado criterio de *expectativa razonable de intimidad.* Por su relevancia a este Informe, a continuación consideramos estos parámetros con detalle. Nuestra evaluación del régimen jurídico aplicable incluirá el estudio de tres asuntos: Primero, consideraremos los contornos *tradicionales* de estas doctrinas. Luego, en segundo lugar, miraremos los retos que la tecnología contemporánea impone a estas normas de derecho tomando en cuenta que en tiempos recientes los Tribunales han mostrado una inclinación a superar las limitaciones de estas doctrinas ante los cambios tecnológicos. Finalmente, como tercer punto, consideraremos los parámetros estatutarios bajo el Stored Communications Act toda vez que, según declarado por el Departamento de Justicia, esta legislación enmarca la conducta investigativa de los actores estatales de Puerto Rico.

1. El Derecho a la Intimidad en Puerto Rico y el Criterio tradicional de la Expectativa Razonable de Intimidad

La Constitución de Puerto Rico no prohíbe todos los registros y allanamientos. Autoriza la expedición de mandamientos judiciales para efectuarlos siempre que

[182] *Arroyo v. Rattan Specialties*, 117 D.P.R. 35, 57-58 (1986) (notas al calce omitidas).

"exista causa probable apoyada en juramento o afirmación, describiendo particularmente el lugar a registrarse, y las personas a detenerse o las cosas a ocuparse".[183] Además, autoriza la realización de registros y allanamientos sin orden siempre que los mismos sean razonables.[184] Lo mismo puede decirse de la Constitución de los Estados Unidos por virtud de la Cuarta enmienda.[185]

De ahí que, todo registro que se haga autorizado mediante orden judicial legítima, se presumirá válido.[186] *Contrario sensu*, todo registro que se realice sin orden judicial, se presumirá inválido, esto es, irrazonable.[187] Ahora bien, el hecho de que no haya orden judicial no quiere decir necesariamente que el acto realizado sea inválido. Recordemos que lo que se prohíbe son los *registros irrazonables.*[188] Por tanto, como cuestión de umbral, hay que determinar primero si ha acaecido un *registro* en el sentido constitucional.[189] Si esto ha ocurrido, se activa la protección constitucional y la presunción de irrazonabilidad, por lo que el Estado viene obligado a demostrar que dicho registro fue *razonable.*[190] Lo razonable en este caso será determinado a partir de un balance entre los intereses apremiantes del Estado y el grado de expectativa razonable a la intimidad que ostente el sujeto registrado.[191] Si en el balance se determina que el registro fue irrazonable, se activa el remedio ofrecido por la Constitución de

---

[183] CONST. E.L.A., art. II, § 10.
[184] *Véase* 1 CHIESA APONTE, *supra* nota 5, § 6.10, en las págs. 356-57 (1991).
[185] 1 CHIESA, *supra* nota 5, § 6.1, en las págs. 280-81 (1991).
[186] Pueblo v. Vázquez Méndez, 117 D.P.R. 170, 177 (1986).
[187] *Véanse Id.*; E.L.A. v. Coca Cola, 115 D.P.R. 197 (1984); 1 ERNESTO L. CHIESA APONTE, DERECHO PROCESAL PENAL DE PUERTO RICO Y ESTADOS UNIDOS, § 6.1, en la pág. 281-82 (1991).
[188] 1 ERNESTO L. CHIESA APONTE, DERECHO PROCESAL PENAL DE PUERTO RICO Y ESTADOS UNIDOS, § 6.1, en la pág. 281 (1991).
[189] 1 JOHN WESLEY HALL, JR., SEARCH AND SEIZURE, § 1:7, en la pág. 14 (2da Ed. 1991 & Supl. 1998).
[190] Pueblo v. Vázquez Méndez, 117 D.P.R. 170, 177 (1986).
[191] 1 CHIESA, *supra* nota 5, § 6.13, en la pág. 406 (1991).

Puerto Rico y por la jurisprudencia federal, esto es, la exclusión de toda consideración judicial de evidencia obtenida en violación de estos preceptos.[192] Si el registro se determina que es razonable, no opera el mencionado remedio. Ahora, si no ha ocurrido un *registro*, entonces –bajo esta doctrina tradicional—no puede hablarse de protección constitucional y por tanto no habría necesidad de demostrar razonabilidad alguna.[193]

Para determinar el elemento de umbral de si hubo o no un *registro* se utiliza el criterio de *expectativa razonable de intimidad.*[194] Esto es, si la persona exhibió una expectativa *razonable* de intimidad al momento de la actividad estatal, ha habido un *registro.* Ahora bien, el criterio de expectativa razonable de intimidad es relativamente reciente ya que surgió en 1967 con el caso de *Katz v. U.S.*[195] Antes de ese caso, la normativa sobre registros y allanamientos se regía bajo otros parámetros. La determinación de si había ocurrido o no un registro en el sentido constitucional se hacía, antes de *Katz*, prestando atención a si había ocurrido una penetración física en áreas constitucionalmente protegidas. Por eso, el énfasis se daba esencialmente al *lugar* registrado.[196] En *Olmstead v. U.S.*,[197] por ejemplo, un caso que trataba sobre el uso de un micrófono (*wiretap*), se determinó que no hubo un registro porque no había habido penetración física y porque no hubo registro o allanamiento de objeto o propiedad como

---

[192] "Evidencia obtenida en violación de esta sección será inadmisible en los tribunales". CONST. E.L.A., art. II, § 10. Para un análisis de la Regla de Exclusión a nivel Federal *véase* 1 JOHN WESLEY HALL, JR., SEARCH AND SEIZURE, §§ 4:1-4:9, en las págs. 141-65 (2da Ed. 1991 & Supl. 1998).
[193] Véanse *Beck v. Ohio*, 379 U.S. 89 (1964); 1 CHIESA, *supra* nota 5, § 6.13, en las págs. 404-05 (1991).
[194] *Katz v. U.S.*, 389 U.S. 347 (1967).
[195] 389 U.S. 347 (1967).
[196] Véanse *U.S. v. Lee*, 274 U.S. 559 (1927); *Olmstead v. U.S.*, 277 U.S. 438 (1928); *Goldman v. U.S.*, 316 U.S. 129 (1942); *Silverman v. U.S.*, 365 U.S. 505 (1961).
[197] 277 U.S. 438 (1928).

tal.[198] Igualmente en *Goldman v. U.S.*[199] se determinó que no hubo un registro en un caso de uso de micrófonos para obtener grabaciones incriminatorias de sospechosos (abogados) de violar las leyes de quiebra porque no hubo una penetración física de los predios, en este caso la oficina de los abogados.

Pero *Katz* revocó estos casos y desplazó el entonces criterio rector de *trespass* por un nuevo paradigma basado en la expectativa razonable de intimidad que ostente el sujeto registrado. Charles Katz fue acusado de violar las leyes federales sobre apuestas al transmitir por un teléfono público información relacionada a sus negocios de apuestas. Agentes federales colocaron micrófonos en la cabina telefónica para grabar lo que él decía en las conversaciones. El asunto, según el tribunal, trascendía consideraciones sobre si la cabina telefónica era o no un área constitucionalmente protegida. Al rechazar la tendencia jurisprudencial previa, el Tribunal Supremo federal estableció la máxima de que

> the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.[200]

Se resuelve que el hecho de que el equipo electrónico utilizado no penetró físicamente la cabina telefónica, no tiene ningún tipo de pertinencia dentro del análisis constitucional.[201] Por tanto, lo realizado por los agentes era un registro para el cual

---

[198] 277 U.S. 438, 464-465 (1928).
[199] 316 U.S. 129 (1942).
[200] *Katz v. U.S.*, 389 U.S. 347, 351 (1967)
[201] Id. en la pág. 353. Es importante notar que el Tribunal en *Katz* explícitamente reaccionó violentamente contra el criterio formalista y rígido de las decisiones previas. De ahí que diga que "It is true that this Court has occasionally described its conclusions in terms of 'constitutionally protected areas,' . . . *but we have never suggested that this concept can serve as a talismanic solution to every Fourth Amendment problem.*" Id. en la pág. 352 n.9 (citas omitidas) (énfasis suplido). Sin embargo, un estudio de los casos sobre este tema

hacía falta obtener una orden judicial.

Ahora, la formulación prevaleciente del criterio rector provino de la opinión concurrente del Juez Harlan:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, *first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'* Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[202]

El legado de *Katz* se resume en los dos principios básicos de la opinión del Tribunal, a saber, (1) que la Constitución protege personas, no lugares; y (2) que lo que una persona, a sabiendas, expone al público no está protegido constitucionalmente. De estos dos principios se desprende la formulación, más articulada, del Juez Harlan que exige la concurrencia de dos requisitos: (1) que el sujeto exhiba una expectativa subjetiva a un derecho de intimidad y (2) que exista una expectativa objetiva de intimidad, esto es, una expectativa que la sociedad esté dispuesta a reconocer como razonable.

El criterio tradicional de *expectativa razonable de intimidad* responde entonces al entendido de que "[c]uando el individuo reclama una expectativa subjetiva a la intimidad en circunstancias bajo las cuales la sociedad no está preparada para reconocer

---

revela cómo la formulación dada a la doctrina de *Katz* realmente se ha tornado en un nuevo *talismán*, quizás más formalista que el anterior.

[202] Id. en la pág. 361 (opinión concurrente del Juez Harlan) (énfasis suplido).

como legítima tal expectativa, lo que se quiere decir es que la sociedad considera razonable y legítima la intrusión, e irrazonable e ilegítimo el reclamo de intimidad".[203] Por eso, aun cuando un sujeto exhiba una expectativa personal de intimidad, si la misma no es objetivamente razonable, se le rechazará su reclamo.[204]

Las dificultades contemporáneas del criterio de expectativa de intimidad son, hoy día, evidentes ante el exponencial incremento en la capacidad Estatal de vigilancia investigativa. En la medida en que se encuentre disponible al público tecnología que permita mayor intromisión, la razonabilidad de cualquier expectativa de intimidad tenderá a disminuirse. Lo que era razonable para Charles Katz, ya no lo es para el ciudadano o la ciudadana del siglo XXI. Cuando Katz caminaba por las calles, no era posible colocar cámaras de vídeo o volar "drones" que grabaran todo momento de la vida cívica en áreas públicas. Tampoco era posible recopilar todas y cada una de las manifestaciones públicas de una persona en su "círculo de amistades", como es posible hoy en las redes sociales. Hoy se puede, y como se puede, teóricamente puede también concebirse como razonable porque constituiría una expectativa que *la sociedad* está dispuesta a tolerar.

Las dificultades obvias de este criterio han sido señaladas por académicos. Por ejemplo, Jeffrey Rosen señala que:

---

[203] I CHIESA, *supra* nota 5, § 6.9, en la pág. 347 (1991).

[204] El *test* de *Katz* fue adoptado en Puerto Rico por *Pueblo v. Lebrón*, 108 D.P.R. 324 (1979). Para determinar si existe una expectativa de intimidad que sea razonable, la jurisprudencia ha requerido que se examinen los siguientes factores, ninguno de ellos determinante: 1) lugar registrado o allanado; 2) naturaleza y grado de la intervención policial; 3) objetivo o propósito de la intervención; 4) si la conducta de la persona era indicativa de una expectativa subjetiva de intimidad; 5) existencia de barreras físicas que restrinjan la entrada o la visibilidad al lugar registrado; 6) número de personas que tienen acceso legítimo al lugar registrado; 7) las inhibiciones sociales relacionadas con el lugar registrado. Véanse, *Pueblo v. Meléndez Rodríguez*, 136 D.P.R. 587 (1994).

> as advances in the technology of monitoring and searching have made ever more intrusive surveillance possible, expectations of privacy have naturally diminished, with a corresponding reduction in constitutional protections.[205]

Asimismo, Meléndez Juarbe ha planteado su insuficiencia para el contexto de tecnologías de información en redes:

> al definirse el contenido de un derecho individual sobre la base de una *expectativa* social, ese derecho se verá reducido -en una especie de espiral descendiente- en la medida en que la sociedad se acostumbre a cierta intromisión con aquello que antes se entendía privado. Es decir, que en la medida que avances tecnológicos nos acostumbren a cierta transparencia, nuestra expectativa de intimidad dejará de ser *razonable,* y, por lo tanto, no protegida por el derecho. Si bien antes podíamos tener una expectativa de que nuestra información personal se mantendría privada, y, por tanto, fuera del alcance del Estado, hoy día esa expectativa es mucho menor tomando en cuenta que una búsqueda en *Google o Facebook* revela tanto sobre nosotros; lo cual implicaría que nuestro derecho a la intimidad queda en la nada solo por vivir en el siglo XXI -si es que nos dejamos llevar por este criterio circular-.[206]

Una postura sensible a estos riesgos debe reconocer que el alcance de los derechos constitucionales debe primar sobre cualquier cambio en la tecnología. Tal vez los derechos constitucionales deben tener la flexibilidad de adaptarse o ajustarse a los

---

[205] *Véase* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60 (2000). Véase además a Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?* 94 COLUM. L. REV. 1751, 1760-61 (1994):

> When used as a factual measure, reliance upon privacy as the centerpiece of Fourth Amendment rights actually creates the potential for less overall privacy protection. This is true most simply because as governmental and nongovernmental intrusions on privacy expand, the scope of what one reasonably expects to be private correspondingly becomes truncated. In other words, because the Court is not asking whether bank or phone records should be kept private (thus invoking privacy as a value), but, rather, whether we as a factual matter expect others to see and use those records (thus viewing privacy as a measurable fact), Fourth Amendment protections will shrink as our everyday expectations of privacy also diminish.

[206] Hiram Meléndez Juarbe, El Derecho a la Intimidad, Nuevas Tecnologías y la Jurisprudencia de Hernández Denton: Lo Público de lo Público, 83 Rev. Jur. Upr 1067 (2014).

cambios. Sin embargo, un reducto mínimo de tales derechos tiene que permanecer inalterado por el auge tecnológico. A tales efectos propone el profesor Rosen:

> A vision of privacy that took seriously the text of the Fourth Amendment might emphasize that there is an irreducible core of constitutional protection against unreasonable searches and seizures of persons, houses, electronic papers, and effects that is necessary for freedom, regardless of how much or how little privacy people subjectively expect in these areas in the light of changing technologies of surveillance.[207]

Por ello, para proteger adecuadamente el derecho constitucional a la intimidad en una controversia referente al tema de la razonabilidad de registros y allanamientos que presente problemas de uso de tecnología, debe evitarse aplicar *mecánicamente* el criterio de adjudicación de *Katz*. Debe procurarse tener, en una mano, la noción de que en Puerto Rico gozamos de una factura más ancha en cuanto al derecho a la intimidad y, en la otra, la noción de que los principios constitucionales no deben estar subordinados a los cambios tecnológicos.

Los adelantos más recientes en la jurisprudencia del Tribunal Supremo de Estados unidos y, particularmente, del Tribunal Supremo de Puerto Rico precisamente apuntan en esta dirección. Tornamos nuestra atención a estos desarrollos.

2. La doctrina de terceros y la expectativa de intimidad ante cambios tecnológicos

Como consecuencia de la visión tradicional sobre la expectativa de intimidad, se puede decir que en general "no hay protección constitucional contra la inspección de objetos que están a la plena percepción de los agentes, siempre que la presencia de los

[207] Véase JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 64 (2000).

agentes en el lugar esté independientemente justificada".[208] Es decir, con relación a lo que hacemos y expresamos a la vista de otros (en una plaza, en la playa, en un parque, en *Facebook*), no tenemos un derecho a la intimidad, según esta visión.

Una manifestación de esta noción tradicional es la llamada doctrina de terceros o "third party doctrine" que atiende aquellas circunstancias en que una persona reclama derechos de intimidad sobre información que ha confiado a otras personas o instituciones (como bancos, plataformas de redes sociales, ISPs o compañías de teléfonos). Según su formulación más tradicional, esta doctrina implica que carecemos de expectativa de intimidad con relación a aquella información que hemos depositado en las manos de otros. Debido a que en el entorno digital nuestra información personal es alojada por muchas entidades que facilitan la conducta en internet (como ISPs y plataformas de redes sociales), la doctrina de terceros ha estado en un proceso de revisión gradual por los tribunales lo cual, a su vez, impacta el alcance del derecho a la intimidad con relación a información depositada en estas instituciones que alojan información.

A través del siglo XX, el Tribunal Supremo Federal desarrolló la doctrina de forma que generalmente negaba expectativa de intimidad a información en manos de tercero. En *United States v. Miller*, 425 US 435 (1976), se resolvió que no existe una expectativa razonable de intimidad en cuanto a las transacciones bancarias, dado que los individuos proveen voluntariamente esa información a los bancos para el manejo de sus cuentas. La decisión dispuso que una *subpoena* para requerir información sobre

[208] 1 CHIESA, *supra* nota 5, § 6.17, en la pág. 434 (1991).

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

Asimismo, en *Smith v. Maryland,* 442 U.S. 735 (1979) se resolvió que no hay una expectativa de intimidad razonable sobre el registro de llamadas realizadas por una persona, pues se espera que las compañías telefónicas tengan acceso a los números marcados. En este caso, se extendió la doctrina de asunción de riesgo de modo que, según el Tribunal Supremo federal, un individuo carece de una expectativa razonable de intimidad con relación el registro de llamadas por haber sido reveladas a terceros. Por tal razón, según este caso, bajo la constitución de los Estados Unidos no es necesario que agentes del orden público soliciten una orden judicial para instalar un artefacto (un "pen register") que capte los números llamados desde un teléfono en particular. Es importante recalcar que el Tribunal en *Smith* subrayó que la información en cuestión (números de teléfono discados) no revela el *contenido* de una comunicación ("a pen register differs significantly from the listening device employed in *Katz,* for pen registers do not acquire the *contents* of communications").

Esta jurisprudencia establece en esa jurisdicción la "doctrina de terceros" de modo que "una persona no tiene una expectativa legítima de intimidad en relación a

información que voluntariamente entregó a un tercero".[209] La misma encierra una noción limitada de lo que constituye el derecho a la intimidad, pues se contrae a proteger aquello que se "guarda en secreto" o lo que está fuera de la vista de otros y no contempla la posibilidad de reclamar el a la intimidad sobre lo que se hace en público. Desde sus inicios fue duramente criticada. Según reseñó el Tribunal Supremo de Puerto Rico en *RDT Construction v, Contralor I*, 141 D.P.R. 424, 437 (1996), citando al tratadista La Fave, "[t]he result reached in *Miller* is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court had developed in *Katz*."

Esta limitada visión, sin embargo, no ha sido adoptada por el Tribunal Supremo de Puerto Rico quien ha tomado en cuenta nuestra tradición constitucional más abarcadora del derecho a la intimidad. Asimismo, el propio Tribunal Supremo de Estados Unidos, en la era digital, ha comenzado a repensar estas premisas, como veremos.

Al mismo tiempo que el Tribunal Supremo federal desarrollaba esta doctrina, el Tribunal Supremo de Puerto Rico adoptó una visión mucho más expansiva sobre el derecho a la intimidad con respecto a información en manos de terceros. Así, en *RDT I*[210] se resolvió que aunque la expectativa de intimidad de las corporaciones "es menor que la que tienen las personas, no por ello están desprovistas de toda protección contra intervenciones irrazonables y arbitrarias por parte del Estado".[211] En particular, en ese

[209] *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979).
[210] 141 D.P.R. 424 (1996).
[211] Id. Pág. 442.

caso se concluyó que una corporación tenía una expectativa razonable de intimidad sobre sus cuentas bancarias, rechazando el razonamiento del Tribunal Supremo en *Miller*.[212]

Sobre las cuentas bancarias, el Tribunal Supremo en *RDT I* expresó que existe una expectativa de intimidad, a pesar de ser información que se entregó a terceros, toda vez que de esta información se puede conocer mucho sobre una persona. A esos efectos, se señaló que:

> Mediante dicha información, se puede determinar la ocupación de la persona investigada, los lugares que frecuenta, los bienes que adquiere, a qué partido o grupo político contribuye, los periódicos y las revistas que lee con frecuencia, la iglesia a la cual hace donativos, las asociaciones a las cuales pertenece, las tiendas y los establecimientos donde compra, los médicos que visita y otra información de naturaleza íntima.[213]

Más recientemente en *Weber v. E.L.A.*, [214] el Tribunal extendió la visión expansiva sobre el derecho a la intimidad, rechazando el razonamiento del caso de *Smith*, y decidió reconocer una expectativa de intimidad sobre el registro de llamadas telefónicas de una persona, aun cuando se encuentre en manos de terceros, por lo que el Estado no puede obtener los registros de estas llamadas sin antes notificarle de ello u obtener una orden judicial a esos efectos. En *Weber*, el Tribunal consideró una solicitud de información por el gobierno, sin orden judicial, a una compañía telefónica de llamadas realizadas a través de teléfonos propiedad del gobierno. En esa solicitud se requirió a la compañía de teléfono (a) el nombre y la información personal de una

---

[212] *Pueblo v. Costas Elenas*, 181 D.P.R. 426 (2011).
[213] 141 D.P.R. 424, 441-442 (1996).
[214] 190 D.P.R. 688 (2014).

persona llamada desde un teléfono oficial y (b) una relación de todas las llamadas realizadas desde ese teléfono por un periodo de un mes.

Al reconocer una expectativa de intimidad sobre el registro de llamadas, el Tribunal expresó que el "rechazo a la doctrina de *Miller* requiere un rechazo similar a la de Smith" ya que "[es] evidente que el registro de llamadas telefónicas permite al Estado adquirir el tipo de información que quisimos proteger en *RDT Cont. Corp. v. Contralor I*".[215] De esa forma, razonó el Tribunal que:

> [a] quién llamamos, cuándo lo llamamos, con qué frecuencia lo llamamos y por cuánto tiempo hablamos equivale, sin duda, a contenido. No cabe duda que hay una expectativa subjetiva de intimidad sobre el registro de las llamadas que hace una persona y que la sociedad entiende que tal expectativa es razonable.[216]

Como con las piezas de un mosaico, dicha información compone pedazos de un rompecabezas que, formado, puede proveer datos de la vida del sujeto sobre los cuales hay una expectativa de intimidad. No obstante, es importante enfatizar una diferencia importante que el Tribunal Supremo destacó en *Weber*. En un caso previo, *Pueblo v. Loubriel*,[217] el Tribunal había resuelto que no se requería orden judicial para que el Estado solicite a un Banco *el nombre* de las personas en cuyas cuentas de banco se habían depositado *cheques emitidos por el propio Estado*, pero que sí se activaba la protección constitucional para obtener acceso a información sobre las transacciones bancarias de esas personas identificadas. Por esto, en *Weber* se resolvió que había sido

[215] 190 D.P.R. 688, 712 (2014).
[216] 190 D.P.R. 688, 712-713 (2014).
[217] 158 D.P.R. 371 (2003).

razonable la solicitud de información (sin orden) del *nombre* de la persona llamada desde un teléfono oficial, mas no de su historial de llamadas. En el caso se explicó que:

> En cuanto a la solicitud del *nombre* del usuario, entendemos que … el Estado tenía derecho a investigar la *identidad* de la persona a quien uno de sus agentes llamó desde su *teléfono oficial* poco antes y durante el operativo. Se trata, pues, de un requerimiento enteramente razonable.... No podemos decir lo mismo en cuanto al requerimiento de entrega de la factura y, con ello, del historial de llamadas del celular.[218]

Nótese que la razonabilidad de las solicitudes sobre la *identidad* de las personas en ambos casos (*Weber* y *Loubriel*) se basó en el hecho de que en ambos casos se solicitó, sin orden judicial, información sobre el uso de artículos que eran propiedad del Estado: dónde se depositaron cheques emitidos por propio el gobierno en *Loubriel*, y llamadas realizadas por teléfonos oficiales, en *Weber*. Es decir, lo anterior no debe interpretarse categóricamente como que el Estado puede evadir requisitos constitucionales porque cuando intenta conocer la identidad de titulares de las cuentas (aunque no solicite información sobre las transacciones).

Lo anterior se hace evidente cuando consideramos el alcance de la jurisprudencia discutida. Al resolverse que las personas tienen una expectativa de intimidad sobre las *transacciones bancarias* y el registro de llamadas telefónicas y, por ende, al rechazar la doctrina de terceros bajo la constitución federal, el Tribunal Supremo de Puerto Rico reconoce protección a información que—aunque independientemente no refleje el contenido de una comunicación—en su agregado refleja suficiente sobre esa persona como para considerarse parte del contenido de sus comunicaciones (como expresa el Tribunal en *Weber*, "equivale, sin duda, a

[218] *Weber v. E.L.A.*, 190 D.P.R. 688, 715 (2014).

contenido"). La extensión de la expectativa de intimidad al *registro de llamadas* representa, a nuestro juicio, una expansión sustancial del derecho a la intimidad en comparación con lo resuelto previamente sobre las transacciones bancarias. Ello, pues las transacciones bancarias son concebiblemente sumamente detalladas y expresivas de patrones o "estilos de vida"[219] de una persona (de ahí la referencia del Tribunal en *RDT I* a que esta información revela detalles sobre bienes que adquiere, periódicos y revistas que lee, asociaciones a las que pertenece y contribuye, médicos que visita, entre otras cosas). En cambio, el registro de llamadas telefónicas, aunque ciertamente revela mucha información de las personas en cuestión (como las personas llamadas así como la frecuencia y duración de llamadas), nunca comprenderá el detalle cualitativo de las transacciones bancarias. Aún con esta diferencia, las protecciones constitucionales se extienden a este tipo de información a partir de *Weber*. Como se verá, lo resuelto en *Weber* encierra implicaciones sustanciales sobre la doctrina de terceros en Puerto Rico, particularmente para un entorno digital toda vez que entidades como ISPs y plataformas de redes sociales alojan una gran variedad de información sobre sus usuarios, que deberá someterse a los lineamientos de nuestra Constitución.

La consecuencia de reconocer una expectativa de intimidad en cuanto a información que está en manos de terceros es, en Puerto Rico, que para que el Estado obtenga esta información **no bastará un requerimiento emitido por *subpoena***. En cambio, ha resuelto el Tribunal, el Estado deberá seleccionar uno de dos procedimientos:

---

[219] *Pueblo v. Loubriel*, 158 D.P.R. 371, 383 (2003).

1- Puede solicitar la información mediante *subpoena*, pero con la obligación de *notificar a la persona de dicha solicitud*. Habiendo sido notificada, la persona puede optar por impugnar el requerimiento en los tribunales.[220]

2- Si el Estado no solicita la información mediante *subpoena*, viene obligado a acudir al tribunal para solicitar una orden judicial autorizando dicha solicitud de información.[221]

Cuando se opta por solicitar la información sin intervención judicial, y se notifica a la persona investigada, esta notificación debe cumplir con los siguientes parámetros constitucionales:

> Dicha notificación deberá ser emitida con razonable anticipación y contener lo siguiente: información específica y detallada que exprese la razón, el propósito y la pertinencia de la solicitud, a la luz de la investigación que se esté llevando a cabo y la disposición legal que faculta a la comisión legislativa en cuestión para realizar tal requerimiento. Lo anterior permitirá que el ciudadano tenga una oportunidad razonable de cuestionar dicho requerimiento ante la autoridad judicial competente, si se siente agraviado.[222]

En cuanto al estándar de evaluación judicial cuando se le solicite una orden (o cuando la persona notificada objete en el tribunal), el criterio dependerá de si se trata, por un lado, de una gestión investigativa de carácter civil o administrativa o, de otro lado, de carácter criminal. Si se trata de una gestión administrativa, impera un criterio de razonabilidad elaborado judicialmente para estos fines.[223] **En cambio, si se trata de**

---

[220] *RDT Construction v. Contralor I* y *Weber v. E.L.A.*, supra.
[221] *RDT Const. Corp. v. Contralor II*, 141 D.P.R. 861 (1996).
[222] *Rullán v. Fas Alzamora*, 166 D.P.R. 742, 778 (2006).
[223] En ese caso, los Tribunales deben evaluar los siguientes criterios: "(1) si la investigación está dentro de la autoridad conferida por ley a la agencia; (2) si el requerimiento no es demasiado indefinido, y (3) si la información solicitada es razonablemente pertinente al asunto específico bajo investigación". Más adelante señala... "Este estándar de pertinencia razonable es menos estricto que el de causa probable utilizado en el ámbito penal. Ahora bien, ... según los procesos administrativos se asemejen más a los de carácter penal, "más se acercarán los dos géneros de registro". Por eso, si el objetivo primario de un registro administrativo es obtener prueba para un proceso penal, la agencia deberá cumplir con los requisitos exigibles en los procesos de índole criminal." *Weber v. E.L.A.*, 190 D.P.R. 688, 703 (2014).

una investigación de carácter criminal los tribunales podrán emitir la orden judicial sólo cuando se demuestre causa probable. Es decir, "mientras más se aleje la investigación de unos fines puramente civiles y más se asemeje a una investigación criminal, aumentará la necesidad de cumplir estrictamente las salvaguardas constitucionales."[224]

Ese rechazo a la doctrina federal no ocurre en un vacío. Como se ha explicado, el rechazo de la doctrina de terceros tiene mucho que ver con el hecho de que nuestra Carta de Derechos es "más abarcadora que la Constitución Federal en lo concerniente a la concesión de derechos, incluyendo el derecho a la intimidad".[225] Haciendo eco de ese principio, el foro local ha manifestado en varias ocasiones que la intimidad, como valor, tiene un "firme arraigo en la cultura de nuestro pueblo" y que esta "goza de un altísimo sitial en nuestra escala de valores".[226] Refleja, además, el entendido de que en nuestra jurisdicción es posible reclamar la protección a derechos de intimidad (al menos en estos casos) *aún con respecto a aquella información que ha estado a la vista de otros* (como las instituciones bancarias o las compañías de teléfono). Esta extensión del derecho de intimidad a información que se ha divulgado se ha dado en otros contextos. Así, según discutido anteriormente, en *Vega v. Telefónica de Puerto Rico*[227] se reconocieron intereses de intimidad en el contexto de grabaciones por cámaras de seguridad en el empleo (por conducta realizada a la vista de todos) que activan mecanismos de control y notificación.

---

[224] *Weber v. E.L.A.*, 190 D.P.R. 688, 703 (2014).
[225] *Pueblo v. Díaz*, 176 D.P.R. 601, 622 (2009).
[226] *E.L.A. v. Hermandad de Empleados*, 104 D.P.R. 436, 445 (1975).
[227] 156 D.P.R. 584 (2002).

En años recientes el Tribunal Supremo Federal ha dado pasos que van reconociendo las limitaciones del criterio de expectativa de intimidad y, en particular, de la doctrina de terceros. En el año 2012, la Jueza Asociada del Tribunal Supremo de Estados Unidos, Sonia Sotomayor, planteó preocupaciones similares en cuanto al criterio de expectativa de intimidad en la era digital:[228] En su opinión concurrente, la Jueza Sotomayor expresó:

> [P]uede que sea necesario reconsiderar la premisa de que un individuo no tiene una expectativa razonable de intimidad con relación a información voluntariamente divulgada a terceras personas.... Este acercamiento no encaja bien con la era digital, pues la gente revela una gran cantidad de información sobre ellos mismos a otras personas en el transcurso de actividades mundanas. La gente revela los números de teléfono que marcan o envían por mensaje de texto a sus proveedores de servicio celular; los enlaces (URLs) de las páginas que visitan y las direcciones de email con las que interactúan son compartidas a sus proveedores de servicio de internet; y los libros, víveres y medicinas que compran, a vendedores en línea. (Traducción suplida)

De forma más contundente, en el 2018, el Tribunal Supremo federal rechazó extender la doctrina de terceros (reconociendo por tanto una expectativa de intimidad) a récords de conexión de teléfonos celulares que reflejan el movimiento de personas bajo vigilancia. En *Carpenter v. United States,* 585 U.S. ___ (2018), el Estado había solicitado información mediante una orden judicial al amparo de la sección 2703(d) del Stored Communications Act (a considerarse *infra*). Esta ley permite que se emitan órdenes judiciales en ciertos casos que no estén fundamentados en causa probable. Se exige que la información solicitada sea meramente "relevante" a una investigación criminal.

---

[228] *U.S. v. Jones*, 132 S. Ct. 945 (2012) (Sotomayor, opinión concurrente).

La información solicitada por el estado (sin orden de causa probable) era data sobre las torres de teléfono celular de una persona durante un tiempo determinado. Con esta información, a base de la localización geográfica de las torres de celular, el Estado pudo establecer un conocimiento aproximado de los movimientos de la persona bajo vigilancia (según reflejados estos movimientos en el lugar de sus teléfonos celulares).

Sin revocar la doctrina de terceros, en una decisión expresamente limitada a sus hechos, el Tribunal se negó a extender el "third party doctrine" a este contexto. Al hacerlo, describió las dificultades de aplicar esta teoría al entorno de las tecnologías contemporáneas, particularmente cuando esta tecnología refleja los movimientos de una persona:

> [W]hile the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records. After all, when *Smith* was decided in 1979, *few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements*.[229]
>
> We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.

Ya el Tribunal Supremo había mostrado preocupación por la tecnología que sea capaz de registrar el movimiento de las personas por periodos prolongados. En *U.S. v. Jones*[230], por ejemplo, se trató sobre el uso de un sistema de GPS en un vehículo, por lo que las preocupaciones en *Carpenter* pueden verse limitadas a este tipo de problema

[229] *Carpenter v. United States*, No. 16-402, 585 U.S. ____ (2018).
[230] *United States v. Jones*, 565 U.S. 400 (2012).

conectado con el rastreo de movimientos personales. De hecho, las preocupaciones del Tribunal en *Carpenter* se suscitan ante lo detallado e intrusivo que puede ser el monitoreo mediante estos mecanismos en un estado de vigilancia perfecta y constante. En ese caso se expresó que:

> A person does not surrender all Fourth Amendment protection by venturing into the public sphere.
>
> ....
>
> A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

No obstante, al así resolver, el Tribunal advirtió contra la aplicación acrítica y automática de la doctrina de terceros ante los cambios tecnológicos ("The Government's position fails to contend with the seismic shifts in digital technology").[231] En el proceso, el Tribunal cuestionó como anacrónica la idea de que con este tipo de tecnología las personas "voluntariamente" divulgan información a las compañías de teléfono, o asumen el riesgo de su divulgación, al expresar que:

> Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. Second, **a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up.** Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. **As a result, in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements.**

[231] *Carpenter v. United States*, No. 16-402, 585 U.S. ____ (2018).

Las preocupaciones del Tribunal Supremo federal con la aplicación de estas normas al entorno digital, son evidentes. Como se ha dicho, el Tribunal Supremo de Puerto Rico, al rechazar la doctrina de terceros en *RDT I* y extender su aplicación en *Weber*, le lleva la delantera al tribunal federal en la protección de derechos de intimidad para este contexto. Con esto, se coloca a los agentes de ley y orden de Puerto Rico en la posición de tener que ajustar su comportamiento a los parámetros constitucionales de nuestra jurisprudencia.

Como se discutió en las determinaciones de hecho de este informe, y según se nos informó por el representante del Departamento de Justicia, los requerimientos de información realizados a plataformas en internet que alojan información de terceros de información se ajustan principalmente a la legislación federal relevante, en particular, el Stored Communications Act. Esta ley, a su vez, está enmarcada en la doctrina de terceros (que en Puerto Rico se ha rechazado). En la medida en que es posible que nuestra Constitución requiera ir más allá de estos parámetros estatutarios, debemos considerar si los actores Estatales en Puerto Rico, al seguir esta legislación, están en violación de derechos constitucionales bajo nuestro ordenamiento.

3. El marco estatutario federal: Stored Communications Act

El Electronic Communications Privacy Act es una ley federal que reglamenta el acceso gubernamental a comunicaciones privadas. El Título II de esta Ley es conocido como el Stored Communications Act o SCA, y específicamente atiende el acceso a comunicaciones electrónicas que son alojadas por entidades como los proveedores de

servicios de internet, así como información mantenida acerca de los suscriptores de servicios de internet, tales como su nombre y dirección de IP.[232] Porque el SCA tiene que ver con información personal alojada en instalaciones de terceros, esta ley está estructurada tomando como punto de partida la doctrina de terceros, antes descrita, ofreciendo en algunos casos mayor protección que la que provee esa doctrina.

Como regla general, los proveedores de servicios de internet y plataformas que alojan comunicaciones electrónicas de personas no deben revelar el contenido de comunicaciones electrónicas, a cualquier persona o entidad, excepto según autorizado por ley. [233] Los gobiernos pueden, según el SCA, solicitar la divulgación de información.

La sección §2703 del SCA regula los requerimientos de información por el gobierno, y los procesos a utilizar para obligar a los proveedores de servicios de internet a entregar información electrónica que almacenan. La ley establece diversos requisitos, dependiendo de si la solicitud de información gira o no en torno al "contenido" de una comunicación, entendido este concepto ("contenido") como "any information concerning the substance, purport, or meaning of that communication".[234]

Cuando el Estado solicita acceso al *contenido* de comunicaciones que están almacenadas **por un periodo de 180 días o menos**, solo podrá obtener esas comunicaciones mediante orden de allanamiento con causa probable. A tales efectos, el organismo gubernamental tiene que dirigir una solicitud a un juez y aportar pruebas

---

[232] 18 U.S.C. §§ 2701, et seq.
[233] 18 USC § 2702(a)(1) ("a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service")
[234] 18 USC § 2510(8)

con fundamentos consistentes para demostrar que existe causa probable para creer que se está cometiendo algún delito. La orden debe ser específica sobre lo que se busca.

Para que se provea el *contenido* de una comunicación electrónica que ha estado en almacenamiento electrónico **por más de 180 días**,[235] el Estado puede solicitarla con una variedad de mecanismos, algunos más laxos que el proceso de orden judicial con causa probable (esto es posible en la jurisdicción federal porque el SCA opera bajo premisas de la doctrina de terceros). El procedimiento dependerá de si se notifica a la persona del requerimiento de información:

(a) *sin notificación a la persona*, la entidad gubernamental puede obtener la información mediante orden judicial con causa probable;[236]

(b) *con notificación a la persona*, se puede obtener la información mediante[237]

1. un *subpoena*, sin orden judicial
2. una orden judicial bajo la sección 2703(d), la cual no requiere causa probable. En cambio, tiene un estándar más laxo que el de una orden judicial estándar. Para obtener la orden, el gobierno debe proporcionar hechos específicos y articulados que demuestren que hay motivos razonables para creer que la información a ser compelida es relevante y material para una investigación criminal en curso.[238]
3. En cualquiera de estos casos, la notificación a la persona puede ser pospuesta por un periodo no mayor de 90 días, de concurrir ciertas circunstancias excepcionales definidas en la ley.[239]

---

[235] Este procedimiento también es aplicable a contenido almacenado por "remote computing services" cuando solo ofrece alojamiento de información (y no otros servicios de comunicación), independientemente de que esté almacenado por menos de 180 días. 18 USC § 2703(b)(2).

[236] 18 USC § 2703(b)(1)(A)

[237] 18 USC § 2703(b)(1)(B)

[238] En *United States v. Warshack*, 631 F.3d 266 (6th Cir 2010) el Sexto Circuito encontró que el mecanismo de orden judicial con algo menos que causa probable es inconstitucional con respecto al contenido de correos electrónicos, aun cuando hayan estado almacenados por más de 180 días toda vez que hay una expectativa de intimidad sobre ese contenido, e independietemente de la doctrina de terceros (la cual no encontró aplicable al contenido del correo electrónico).

[239] 18 USC § 2705. para poder ejercer esa disposición, debe probar que la demora era necesario para prevenir: daño a la vida, la seguridad de un individuo, para impedir una fuga, impedir destrucción de evidencia o la intimidación de testigos o que notificar a la persona pone en riesgo la investigación.

Si, en cambio, la información solicitada **no es sobre el contenido de comunicaciones** (lo que el Departamento de Justicia de Puerto Rico llamó en la Audiencia Pública "información transaccional") la SCA tiene una serie de reglas especiales para obligar el descubrimiento de cierta información básica de suscriptores con menores garantías procesales.

Por un lado, en general la información "transaccional" que no es de contenido puede obtenerse mediante:[240]

(a) Orden judicial con causa probable;
(b) Orden judicial bajo el estándar menor de la sección 2703(d) (motivos razonables para creer que la información a ser compelida es relevante y material para una investigación criminal en curso)
(c) Con el consentimiento de la persona.

Cabe señalar que este fue precisamente el tipo de asunto que el Tribunal Supremo federal consideró en *Carpenter*, con relación a la información sobre las torres de teléfono celular de una persona. Por considerarse que había una expectativa de intimidad sobre esta información, la orden judicial de menor estándar de la sección 2703(d), fue insuficiente.

Ahora bien, hay cierta información sobre suscriptores que puede obtenerse mediante *subpoena*, **sin intervención judicial alguna**. Lo que se conoce como "información básica de suscriptores" incluye:[241]

(a) Nombre
(b) Dirección
(c) Registros de llamadas locales y de larga distancia o registros de tiempos de sesión y su duración

[240] 18 USC § 2703(c)(1)
[241] 18 USC § 2703(c)(2)

(d) Tiempo de servicio (incluyendo fecha de comienzo) y tipos de servicios utilizados.
(e) Número de teléfono u otra información de suscripción identidad, incluyendo cualquier dirección de red asignada
(f) Formas de pago y fuentes de pago para tal servicio (incluyendo tarjeta de crédito y número de cuenta de banco)

Como puede apreciarse, hay una variedad de circunstancias en el SCA en las que puede requerirse información sin que medie una orden con causa probable. Ello incluye, la llamada información básica de suscriptores (que puede obtenerse por *subpoena*); toda la información que no es de contenido (que puede obtenerse con una orden de menor estándar bajo la 2703(d)) e inclusive información de contenido almacenada por más de 180 días con notificación (mediante *subpoena*, o con orden de la sección 2703(d)). Este esquema refleja un tratamiento compatible con la doctrina de terceros en la medida en que presupone que la información almacenada por terceros carece de expectativa de intimidad y, por tanto, es suficiente algo menos que causa probable. Sabemos, sin embargo, que bajo la Constitución de Puerto Rico el estándar es más alto requiriéndose orden judicial con causa probable o notificación (en cuyo caso hay oportunidad para que la persona impugne en un tribunal y se dilucide si hay causa probable).

Así, por ejemplo, con relación a la llamada información básica que no es de contenido y es obtenible mediante *subpoena* bajo el SCA (y que se informó a esta Comisión se solicita en Puerto Rico sin intervención judicial como información "transaccional"), es cuestionable que la misma pueda ser obtenida mediante *subpoena* sin violentar la norma de *Weber* y la jurisprudencia de nuestro Tribunal Supremo.

Tómese, por ejemplo, los records de un suscriptor ante un ISP. No cabe duda de que este es el tipo de información para la cual sería necesario activar las protecciones constitucionales bajo nuestra jurisprudencia más abarcadora. De hecho, así lo hizo el Tribunal Supremo de Nueva Jersey en *State v. Reid.*[242] En ese caso el Tribunal consideró una situación en que el Estado había conseguido la dirección de IP de una persona y, con ella, requirió al ISP que bridara la información asociada al usuario de esa dirección de IP; es decir: dirección, número de teléfono, tipo del servicio, dirección de IP dinámica provista al usuario, número de cuenta, dirección de correo electrónico y método de pago. Tras analizar su jurisprudencia constitucional, el tribunal de Nueva Jersey resolvió que la Constitución de ese estado "protects an individual's privacy interest in the subscriber information he or she provides to an Internet service provider."[243] Por esa razón, el Tribunal de Nueva Jersey requirió los mecanismos procesales apropiados a estos casos según su Constitución (en esa jurisdicción es suficiente el *grand jury subpoena*). Al así resolver, el tribunal declaró:

> ISP records share much in common with long distance billing information and bank records. All are integrally connected to essential activities of today's society. Indeed, it is hard to overstate how important computers and the Internet have become to everyday, modern life. Citizens routinely access the Web for all manner of daily activities: to gather information, explore ideas, read, study, shop, and more.
>
> Individuals need an ISP address in order to access the Internet. However, when users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential. Many are unaware that a numerical IP address can be captured by the websites they visit. More sophisticated users understand that that unique string of numbers, standing alone, reveals little if anything to the outside world. Only an Internet service provider can translate an IP address into a user's name.

[242] 194 N.J. 386, 945 A.2d 26 (2008).
[243] *State v. Reid*, 194 N.J. 386, 399, 945 A.2d 26, 33–34 (2008).

> In addition, while decoded IP addresses do not reveal the content of Internet communications, subscriber information alone can tell a great deal about a person. With a complete listing of IP addresses, one can track a person's Internet usage.[244]

Lo anterior contrasta con lo dispuesto en la Orden General más reciente de la División de Crímenes Cibernéticos, Orden General 600-613, aprobada el 25 de abril de 2018, la cual establece que cierta información podrá obtenerse mediante *subpoena* (consistente con el texto de la SCA con respecto a información básica de suscriptores). El texto de esta sección se reproduce en la sección de hallazgos de este informe,[245] aunque destacamos que su Parte I(10) permite el requerimiento mediante *subpoena* de la dirección de IP de un usuario, así como dirección de correo electrónico, número de teléfono, registros de conexión telefónica y duración de llamadas, modo de pago incluyendo número de tarjeta de crédito, nombre y dirección.[246]

Aunque el Tribunal Supremo no ha atendido específicamente este tipo de circunstancias, resulta claro que la jurisprudencia descrita apunta en esta dirección, por

---

[244] *State v. Reid*, 194 N.J. 386, 398, 945 A.2d 26, 33 (2008).

[245] Supra Parte IV(B).

[246] Notamos que lo aquí discutido se limita a información *almacenada* y no a la *interceptación* de información (sea o no de contenido). Con respecto a la interceptación información sobre comunicaciones que *no es de contenido*, el llamado Pen Register Act permite instalar artefactos que recojan prospectivamente metadata digital sobre comunicaciones (no almacenada), incluyendo "routing, addressing, or *signaling information*" generada por tecnología de internet mediante una orden judicial menor a causa probable (es decir, una orden a base de que la información sea relevante a una investigación criminal). 18 USC § 3121-3123. Este sería el caso, por ejemplo, de la interceptación de metadata sobre comunicaciones por email como los "headers" que contienen emisor, receptor, Dirección IP, fecha de envío y recibo, entre otras cosas. Por las mismas razones articuladas en este informe, las agencias de ley y orden en Puerto Rico deben cumplir con los parámetros constitucionales de causa probable para este tipo de intervención que, aunque semánticamente pueda decirse que no es contenido, claramente está contemplada por la jurisprudencia constitucional en nuestra jurisdicción. Después de todo para el contexto digital, el "routing, addressing, or signaling information" es en cierto modo análogo a los números marcados por un teléfono y que en *Weber*, *supra*, se resolvió que sólo pueden obtenerse mediante procedimientos con garantías superiores. Nótese que el Pen Register Act permite a los estados (y a Puerto Rico) solicitar esta orden judicial de menor categoría para instalar estos artefactos, *a menos que lo prohíba el derecho estatal*, lo cual es el caso en Puerto Rico como cuestión constitucional según discutido en este informe. *Véase* 18 USC § 3122(b) ("*Unless prohibited by State law*, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device").

lo cual los procedimientos de la Policía y del Departamento de Justicia deben revisarse a la luz de estos criterios. En el entorno digital esta preocupación es particularmente importante: toda la conducta de las personas en la internet es facilitada por instituciones que cumplen diversos roles en la infraestructura de la red. Ya sean plataformas de redes sociales, ISPs, servidores de internet, entre otros, todas estas piezas de la comunicación en línea constituyen espacios de potencial intervención estatal y son, de facto, repositorios de información personal.[247] Como recientemente expresó un académico en el campo: "[w]e face a future in which active surveillance is such a routine part of business that for most people it is nearly inescapable… There is good reason to believe that, if nothing is done, gratuitous surveillance will be built into nearly every business and business model."[248] En un entorno digital en que la información privada es constantemente recopilada, analizada, mercadeada y utilizada para una variedad de fines, es necesario que las normas constitucionales aplicables al acceso gubernamental a esta información (y las políticas institucionales pertinentes) se mantengan relevantes a esta realidad.

A tales efectos, para que los requerimientos de información cumplan con los parámetros constitucionales—ya sea información básica de suscriptores de ISPs así como información análoga o más detallada que almacenen los ISPs o que alojen terceros como servicios de redes sociales sobre los usuarios (como puede ser, por

---

[247] Véase JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006); Hiram Meléndez Juarbe, *Intermediarios y Libertad de Expresión: Apuntes para una conversación, en* HACIA UNA INTERNET LIBRE DE CENSURA: PROPUESTAS PARA AMÉRICA LATINA, CENTRO DE ESTUDIOS EN LIBERTAD DE EXPRESIÓN Y ACCESO A LA INFORMACIÓN, Universidad de Plermo, Buenos Aires (2012).

[248] Tim Wu, *How Capitalism Betrayed Privacy*, The New York Times, 10 de abril de 2019, https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html

ejemplo, el historial de tráfico o de uso de una persona)[249]—, estas solicitudes deben estar precedidas por una orden judicial basada en causa probable o, en la alternativa, un requerimiento por *subpoena* junto a una notificación previa a la persona investigada.[250]

Debemos subrayar que, de optarse por el mecanismo de *subpoena* con notificación, no basta con que la entidad que aloja la información tenga como política avisar voluntariamente a las personas de este hecho.[251] Es responsabilidad del Estado

---

[249] Según se consideró en la porción de hallazgos, *supra* Parte IV(B), la Orden General pertinente no establece si el historial de visitas almacenadas por un proveedor de servicios (URLs visitados) debe considerarse como "contenido". Evidentemente, dada nuestra jurisprudencia y por la naturaleza expresiva de esta información, ello sólo debe obtenerse mediante orden judicial de causa probable y no mediante *subpoena* ni mediante orden judicial de menor categoría bajo la § 2703(c)(1). Después de todo, el historial de visitas en internet se parece a, y refleja mucho más que, los números marcados por un teléfono que consideró el Tribunal Supremo en *Weber*, *supra*. Como articuló el profesor Daniel Solove:

> On the surface, a list of IP addresses is simply a list of numbers; but it is actually much more. With a complete listing of IP addresses, the government can learn quite a lot about a person because it can trace how that person surfs the Internet. The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's sexual fetishes and fantasies, her health concerns, and so on.
>
> Perhaps even more revealing are URLs. A URL is a pointer--it points to the location of particular information on the Internet. In other words, it indicates where something is located. When we cite to something on the Web, we are citing to its URL. For example, the following is the URL to Orin Kerr's webpage: http://www.law.gwu.edu/faculty/profile.asp?ID=3568.
>
> One can visit Kerr's webpage by typing the above URL into one's web browser and clicking the "Go" button. Therefore, URLs can reveal the specific information that people are viewing on the Web. URLs can also contain search terms. So if one does a search on Google for Orin Kerr, she will be directed to a URL that reads: http://www.google.com/search?hl=en&ie=UTF-8&oe=CUTF-8&q=orin+kerr.

Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 GEO. WASH. L. REV. 1264, 1287 (2004).

[250] Nótese que, incluso en el contexto de la litigación privada, cuando un demandante busca la identidad de demandado a través de su Dirección IP los tribunales aseguran celosamente que no se vulneren los derechos de anonimato antes de autorizar su identificación. Véase Doe I v. Individuals, Whose True Names are Unknown, 561 F.Supp. 2d 249 (D. Conn. 2008) (requiriendo previo a la divulgación de la identidad de un demadnado "that a plaintiff make a concrete showing as to each element of a prima facie case against the defendant"); Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1092, 1097 (W.D. Wash. 2001) ("Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas[;] . . . the constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded.")

[251] La Orden General más reciente de la División de Crímenes Cibernéticos, Orden General 600-613, aprobada el 25 de abril de 2018 resalta que, para la información básica de suscriptor, las entidades que guardan la información habitualmente notifican a los usuarios. *Véase* Parte I(10)(g) ("La ley federal establece que aunque la entidad gubernamental que recibe la información solicitada mediante *subpoena*, no está obligada a proporcionar aviso a un suscriptor o cliente. Dicho esto, internamente las compañías proveedoras de comunicación electrónica podrían notificar a su cliente sobre la petición de información de registro.")

proveer esta notificación, bajo los criterios establecidos jurisprudencialmente, o—en la alternativa—solicitar orden judicial.

Por tanto, en la medida en que la práctica investigativa en Puerto Rico aspira a ajustarse al SCA, pero no a los dictámenes de la protección constitucional más exigente de nuestra Constitución, opera una violación al derecho constitucional a la intimidad.[252]

[252] Notamos que el Tribunal de Circuito Federal para el Primero Circuito, en *Telecommunications Regulatory Bd. of Puerto Rico v. CTIA-Wireless Ass'n*, 752 F.3d 60 (1st Cir. 2014) resolvió (bajo circunstancias muy específicas) que el SCA ocupó el campo con respecto a una ley de Puerto Rico muy puntual. En ese caso se consideró que la ley federal contiene una prohibición expresa a que compañías de telecomunicaciones divulguen información de usuarios (a menos que se cumplan ciertos procedimientos), mientras que la ley de Puerto Rico requería tal divulgación (sin procedimiento alguno). Esto colocaba a la ley de Puerto Rico en conflicto directo con la ley federal porque las compañías de telecomunicaciones estaban en la posición de tener que violar la ley federal por cumplir con la ley de Puerto Rico. Ausente una disposición expresa de campo ocupado en el SCA, el Tribunal atendió el caso bajo la doctrina de "conflict preemption" la cual se activa cuando, como en ese caso, "compliance with both state and federal law is impossible". *Id.* Este no es el caso con las garantías constitucionales más exigentes impuestas de nuestra Constitución, toda vez que cumplir con el derecho constitucional de Puerto Rico no incumple la ley federal. De hecho, la propia SCA expresamente autoriza requerimientos de información con exigencias mayores. El SCA permite que una entidad gubernamental estatal solicite la información básica de suscriptores no solo mediante *subpoena* sino también mediante cualquier procedimiento estatal más riguroso (como una orden judicial basada en causa probable). Véase 18 USC § 2703(c)(2) (autorizando la divulgación "…when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena *or any means available under paragraph (1)*". El inciso (A) del mencionado párrafo (1) incluye, entre otras posibilidades, una orden judicial con causa probable autorizada por el derecho estatal: "a warrant … *using State warrant procedure*"). Asimismo, la sección 2703(d) (permitiendo órdenes judiciales con menos que causa probable para ciertos casos) reconoce la protección mayor que puede dar un estado al derecho a la intimidad, al no permitir que se utilice la orden judicial menor de la 2703(d) cuando ese tipo de orden no esté autorizada por el derecho estatal. 18 USC § 2703(d) ("In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State"). Además del caso de *Reid* (que asume sin discutir que la constitución de Nueva Jersey no está desplazada por la SCA) otras jurisdicciones han concluido que la ECPA no desplaza la legislación estatal del campo que regula. *Véase* Valentine v. NebuAd, Inc, 804 F Supp. 2d 1022, 1029 (2011); In re National Security Agency Telecomm'ns Records Litig., 483 F. Supp. 2d 934, 939 (N.D. Cal. 2007).

VII. Conclusiones

En vista de los hallazgos y determinaciones de hechos en este informe, así como del análisis jurídico elaborado, la Comisión de Derechos Civiles emite las siguientes Conclusiones. Estas conclusiones se elaboran tomando como punto de partida dos principios básicos.

Primero, y como se ha resaltado a través de este informe, rechazamos la noción de que, sólo porque algo que ocurre a la vista de todos y todas no es posible hablar de derechos con respecto a esa conducta pública. El derecho al anonimato en torno a lo que se hace en público es fundamental para controlar el riesgo de vigilancia selectiva y se entremezcla con los derechos de intimidad, participación política en una democracia, así como con el interés de asociación libre con otras personas. El Tribunal Supremo de Puerto Rico así lo ha reconocido al exigir controles a sistemas de vigilancia por cámaras (aún en espacios a la vista de otras personas) y, además, al rechazar reiteradamente la norma federal conocida como la "doctrina de terceros", según discutido en este informe. Es indispensable que nuestro sistema de derecho y la Policía asuman esta postura para minimizar aquellas condiciones que apuntan a la creación de un efecto disuasivo o "chilling effect" en el ejercicio de libertades civiles. Esto, además, se sustenta en la noción clave de que en Puerto Rico gozamos de una factura más ancha en cuanto al derecho a la intimidad.

Segundo, nuestras conclusiones se sustentan en la noción de que los principios constitucionales y de derechos humanos no deben estar subordinados a los cambios tecnológicos. Conforme a esta postura, el profesor Tribe comenta lo siguiente:

> [T]he Constitution's norms, at their deepest level, must be invariant under merely technological transformations. Our constitutional law evolves through judicial interpretation, case by case, in a process of reasoning by analogy from precedent. At its best, that process is ideally suited to seeing beneath the surface and extracting deeper principles from prior decisions. At its worst, though, the same process can get bogged down in superficial aspects of preexisting examples, fixating upon unessential features while overlooking underlying principles and values.[253]

Debemos asegurar que la protección de los derechos humanos no quede sacrificada en el altar del desarrollo tecnológico. La tecnología contemporánea facilita acceso a una gran variedad de información sobre las personas (tanto en nuestras interacciones públicas como en las privadas) pues ha cambiado la arquitectura tecnológica que antes dificultaba obtener esta información. Pero, por el hecho de que hoy cierta vigilancia es *posible*, no debe llevar a la conclusión de que es admisible. Para evitar el deslizamiento desde lo que *es* a lo que *debe ser* es, por tanto, indispensable resaltar aquellos principios constitucionales y derechos humanos que se pueden ver socavados por el cambio tecnológico.

La Comisión de Derechos Civiles concluye que, durante el periodo bajo investigación y en particular alrededor de los eventos de protesta pública del 1 de mayo de 2017, la Policía de Puerto Rico exhibió una carencia de controles y estructuras institucionales apropiadas para evitar el abuso discriminatorio de las prácticas de vigilancia en el contexto de la protesta pública, ya sea a través de la internet o presencialmente. Ausentes mecanismos de control vigorosos, la tecnología digital contemporánea hace posible que la vigilancia constitucionalmente cuestionable sea

---

[253] Laurence H. Tribe, *The Constitution in Cyberspace*, http://swissnet.ai.mit.edu/6095/articles/tribe-constitution.txt

indetectable en muchos casos y permanezca impune. Ciertamente en los últimos meses, mientras esta Comisión investigaba la querella que da lugar a este informe, la Policía enmendó algunas de sus políticas para ajustar ciertos procedimientos. No obstante, la realidad es que la Policía de Puerto Rico carece de parámetros reales y efectivos y las nuevas políticas, por sí solas, no garantizan que no continúen manifestándose elementos de una cultura institucional inadecuada desde el punto de vista de la protección de derechos.

Ante este cuadro, el riesgo de vigilancia selectiva inconstitucional es intolerablemente alto pues –en todas las etapas del proceso (desde la recopilación de información, hasta los protocolos para su preservación y disposición)— existen amplias oportunidades para el abuso de estos mecanismos. Ante la historia reciente de persecución política en este país, resulta imperativo que las instituciones de vigilancia policiaca de Puerto Rico sean repensadas en toda su extensión desde una perspectiva de derechos humanos.

En vista de todo lo contenido en este informe, esta Comisión concluye que las prácticas y políticas del Negociado de la Policía de Puerto Rico relacionadas con la vigilancia y el monitoreo en el contexto de actividades de protesta pública violentan los derechos de libertad de expresión, asociación e intimidad de las personas.

A continuación, describimos los elementos principales de esta conclusión, en las cuatro áreas principales de este informe.

(a) ***Con relación a las prácticas de monitoreo por parte de agentes de orden público en redes sociales.***

Esta Comisión cuestiona la legitimidad de las expresiones de la Superintendente de la Policía emitidas días antes de las manifestaciones del 1 de mayo de 2017, por el efecto disuasivo ("chilling effect") que ese tipo de manifestación tiene sobre el derecho a la libertad de expresión y asociación. Ante esta Comisión se pretendió justificar las manifestaciones de la Superintendente sobre la base de que los alegados comentarios en Facebook apuntaban a la posible comisión de delitos. No obstante, no se brindó a esta Comisión información de tales comunicaciones, ni de su naturaleza delictiva.

Se informó a esta Comisión que la Policía de Puerto Rico no realizaba monitoreo afirmativo de personas en las redes sociales y que solo actuaba reactivamente, o sea, luego de recibir información en su página de Facebook o a través de otras fuentes. Sin embargo, al no existir constancia de las expresiones que alegadamente motivaron el monitoreo de las redes sociales, esta Comisión carece de evidencia que permita darle credibilidad o validez a la conducta pública de la Superintendente que, sin duda, es el tipo de conducta oficial que impacta el disfrute de los derechos humanos. En estas circunstancias existe un alto riesgo de que las advertencias públicas de las Superintendente hayan contribuido a crear un ambiente de temor en torno a las actividades de vigilancia de la Policía de Puerto Rico, inclusive sobre la conducta expresiva lícita. Independientemente de la participación, que en efecto, haya habido en las referidas protestas, el hecho de que en la conciencia colectiva está plantada la confirmación de una vigilancia de la conducta expresiva constitucionalmente protegida,

plantea un riesgo duradero y persistente sobre el derecho a la libertad de expresión y asociación.

Existe prueba de referidos por la Policía de Puerto Rico al FBI en torno a expresiones en Facebook que la Policía entendió eran "amenazantes" (que ocurrieron posterior a las manifestaciones públicas de la Superintendente). No obstante, según se discutió en este informe, muchos de estos referidos al FBI versaron sobre expresiones que están constitucionalmente protegidas por tratarse de hipérbole política y porque no constituyen una incitación a la violencia de aquellas que constitucionalmente pueden prohibirse. Es decir, la Policía de Puerto Rico refirió al FBI a personas por discutir en Facebook asuntos de interés público que, incorrectamente, interpretó como amenazantes. Recordamos que sólo la llamada "amenaza real", y no la expresión política cruda de carácter agresivo, es la que se puede prohibir como cuestión constitucional. Por esto, resulta además altamente cuestionable que el FBI haya procesado criminalmente a una persona (con cargos que eventualmente fueron desestimados) por expresiones en redes sociales de dudosa caracterización como amenazantes. Resulta igualmente cuestionable que las agencias federales hayan utilizado esa acusación para divulgar en los medios este proceder a sólo días de las manifestaciones del 1 de mayo de 2017. En estas circunstancias, también resalta el riesgo de que las agencias de ley y orden en la jurisdicción federal estén provocando un temor público sobre la vigilancia gubernamental con el efecto de inhibir la libertad de expresión.

Considerando el nefasto historial de nuestras instituciones públicas con respecto al abuso de los mecanismos de vigilancia, unido a las capacidades tecnológicas

contemporáneas de supervisión (y el conocimiento público, aunque general, de estas capacidades) es particularmente preocupante el riesgo de este "chilling effect" disuasivo de la expresión legítima.

Según hemos expuesto previamente, subrayamos que es irrelevante el que la conducta observada en las redes sociales haya ocurrido en público a la vista de terceros. Los derechos de expresión anónima, libertad de expresión y asociación se ven profundamente afectados cuando se normaliza el panóptico y la vigilancia.

Precisamente para atender riesgos en torno al derecho a la intimidad y la dignidad humana, el Tribunal Supremo de Puerto Rico ha requerido ciertos elementos de control, incluso para casos en los que se vigile la conducta que ocurre en público. Por esto, el hecho de que se haya realizado monitoreo en redes sociales sin que se haya dejado rastro alguno de esa actividad, ni registro que facilite la verificación de la legalidad de dicho monitoreo, presenta un defecto crítico en la forma en que la Policía de Puerto Rico asumió su gestión. Si bien la Policía de Puerto Rico nos informó que la vigilancia en redes sociales que dieron base a las expresiones públicas de la Superintendente fueron en *reacción* a información recibida, la realidad es que no existe constancia de estos referidos. La informalidad con la que se asumió esta información alegadamente recibida acusa un problema mayor de una cultura institucional en las gestiones de vigilancia carente de controles que abre paso a los riesgos de abuso que hemos visto en la historia de este país.

Lo anterior resalta la necesidad identificada a través de este informe de que existan parámetros y controles reales a la discreción de los programas estatales de vigilancia. Independientemente de que podamos catalogar una situación particular

como visible ante terceros o sobre la cual no hay una expectativa razonable de intimidad porque ocurre a la vista de todas y todos, es indispensable evitar el mal uso y abuso de estas facultades.

(b) ***En torno a las prácticas de recopilación de información privada digital durante el ejercicio de funciones investigativas***

Según se desprende de esta investigación, existe una profunda confusión tanto en la Policía de Puerto Rico como en el Departamento de Justicia en torno a los límites constitucionales que rigen la solicitud de información personal que es alojada por terceros. Resaltamos que la gran mayoría de la información personal (y que se genera con el mero uso de plataformas en internet) es almacenada por entidades que facilitan esta actividad individual (ya sea servicios de redes sociales, ISPs, o cualquier otro intermediario que hace posible la conducta en internet). Por tanto, resulta vital que los operadores estatales en Puerto Rico se atengan a los parámetros más estrictos de nuestra jurisprudencia en cuanto a la solicitud de información personal a estos terceros. Según nuestra jurisprudencia, las personas pueden tener una expectativa de intimidad con relación a información personal que está en manos de terceros, por lo que es indispensable que se cumplan con ciertas garantías procesales constitucionalmente requeridas.

Según discutido en este informe, el Departamento de Justicia de Puerto Rico se deja llevar por el régimen estatutario federal (el Stored Communications Act) para solicitar la información personal que es alojada en servidores de terceros: cuando se trata de información catalogada como transaccional (que no es contenido de comunicaciones) se solicita por medio de *subpoena*. Por otro lado, cuando se trata del

contenido de una comunicación, se solicita mediante orden judicial. El régimen estatutario federal, sin embargo, tiene como base la llamada *doctrina de terceros* la cual sostiene que no hay una expectativa de intimidad con relación a información personal que está alojada por terceros. No obstante, nuestro Tribunal Supremo ha rechazado esta doctrina para una variedad de circunstancias, debido a que en Puerto Rico el derecho a la intimidad es más abarcador que su equivalente en la jurisdicción federal. Y, aunque se nos informó en vista pública que las prácticas del Departamento de Justicia se atemperan a la jurisprudencia de Puerto Rico, ese Departamento se negó a brindar documentación que articulara estos procedimientos. En cambio, la Orden General más reciente de la División de Crímenes Cibernéticos del Negociado de la Policía mantiene la postura de que esta información llamada "transaccional" será solicitada sin orden judicial, mediante *subpoena* y sin notificación a la persona.

A pesar de que el Tribunal Supremo no ha atendido específicamente este tipo de circunstancias, resulta claro que la jurisprudencia considerada en este informe apunta a que los procedimientos de la Policía y del Departamento de Justicia deben revisarse. A tales efectos, para que los requerimiento de información cumplan con los parámetros constitucionales—ya sea información básica de suscriptores de ISPs así como información personal análoga o más detallada que almacenen los ISPs o que alojen otras entidades como servicios de redes sociales (como puede ser, por ejemplo, el historial de tráfico o de uso de una persona)—, estas solicitudes deben estar precedidas por una orden judicial basada en causa probable o, en la alternativa, en un requerimiento por *subpoena* junto a una notificación previa a la persona investigada. De optarse por el mecanismo de *subpoena* con notificación, no basta con que la entidad

que aloja la información tenga como política avisar voluntariamente a las personas de este hecho, pues es responsabilidad del Estado proveer esta notificación.

(c) En cuanto a la grabación de actividades de protesta pública con cámaras de video y audio

Las prácticas de grabación de eventos públicos de la Policía de Puerto Rico presentaron a esta Comisión preocupaciones de diversa índole.

Primero, encontramos serias deficiencias en términos de *controles administrativos* internos que permitan evaluar sistemáticamente el trabajo de la Unidad Técnica de Grabaciones y, por ende, verificar el cumplimiento con obligaciones constitucionales. A estos efectos, no encontramos registro, bitácora u otro tipo de récord sistemático sobre las actividades que se graban, ni auditorías internas sobre las grabaciones que se recopilan. Asimismo, no existió durante todo el periodo bajo evaluación un registro de los oficiales asignados a cada tarea o evento.

Sobre este aspecto, es pertinente notar los señalamientos del Asesor Técnico de Cumplimiento, en torno a los videos del 1ro de mayo de 2017 captados por la Sección Técnica de Grabaciones. En su informe, encontró deficiencias en el sistema de archivo de los videos toda vez que su numeración (usualmente generada secuencialmente por las cámaras de video), reflejaba archivos omitidos (números ausentes de la secuencia), lo cual arroja dudas en torno a si finalmente se guardaron todos los videos captados y, por ende, en torno a la selectividad del material preservado.

Segundo, encontramos cierta *vulnerabilidad de los videos a ser editados o borrados selectivamente*. La Orden General sobre la grabación de eventos públicos vigente al momento de los eventos del 1 de mayo contenía una norma de preservación

e integridad del material: los videos debían ser mantenidos por un periodo de dos (2) años, luego de lo cual debían ser borrados, a menos que se determinara que contienen "actividad delictiva", o si forman parte de alguna investigación o procedimiento judicial o administrativo. Actualmente, la nueva Orden General establece un término de preservación de cinco (5) años para videos que se identifiquen como que contienen actividad delictiva (o indefinido si son parte de un proceso judicial o administrativo), o de un (1) año si no contienen actividad delictiva, al cabo del cual deben borrarse. En ningún momento se hace mención en estas políticas a la posibilidad de borrar selectivamente material antes de los términos dispuestos, por razón alguna.

No obstante, en la Inspección Ocular en las oficinas de CRADIC se nos indicó que, cuando se somete el video grabado por técnicos o agentes de la Sección Técnica de Grabaciones, en la División se borra o elimina contenido que la Policía entiende carece de importancia evidenciaria o que no revela información sobre la comisión de delitos. Se expresó, además, que después de esta revisión (y eliminación de contenido si es necesario) es que se almacena contenido en los servidores. Asimismo, al preguntarse si los videos relacionados con las protestas del 1 de mayo de 2017 han sido editados de alguna forma (incluyendo, pero sin limitarse a, borrar contenido, modificar el orden de eventos captados, añadir videos de otras fuentes), se contestó que "se edita toda actividad no criminal". Resaltamos, los hallazgos del Informe del Asesor Técnico, toda vez que identificó al menos un grupo de videos que a todas luces fue sustancialmente editado. Ese informe describió porciones de videos que se entrelazaban entre sí de forma traslapada, de modo que por instantes se percibían y escuchaban simultáneamente.

Tercero, en torno al *equipo utilizado por la Sección Técnica de Grabaciones*, como se ha dicho, esta Comisión pudo comprobar la adquisición por la Policía de Puerto Rico de varios "drones" (vehículos aéreos no tripulados), sin que su uso esté regulado por esa agencia. No existe protocolo ni Orden General que atienda las particularidades de este tipo de tecnología. A pesar de informarse por escrito a esta Comisión que se había adquirido un solo *drone,* en su visita a las oficinas de CRADIC se pudo observar la existencia de al menos cuatro (4) *drones*, equipados con cámara de grabación marca DJI, Modelo Phantom 3 Standard. Estos equipos tienen la capacidad de elevarse a 120 metros de altura y tienen la capacidad de grabar en áreas claramente cobijadas por una expectativa razonable de intimidad, como sería el caso de observar a través de ventanas en edificios residenciales. Todo ello sin que exista reglamentación especial en la Policía que atienda los retos específicos que esta tecnología presenta.

Cuarto, existe *falta de claridad en cuanto a los criterios para determinar qué actividad o evento se grabará.* Al preguntarse específicamente sobre los criterios que se utilizan para peticionar que determinado evento sera grabado, se nos planteó por escrito que esa decisión se rige por "la sana discreción del Comisionado". Al mismo tiempo, se nos planteó que "de grabarse algún evento, dicho evento se graba en su totalidad durante el evento en particular, hasta que culmine el evento". No obstante estas representaciones, durante la Inspección Ocular en las oficinas de CRADIC se planteó a esta Comisión que la decisión de grabar un evento respondía a una determinación de si hay riesgo de que acontezcan "actos criminales o violaciones de derechos civiles". Lo anterior revela una amplia discreción, y por ende, potencial de

selección carente de criterios manejables, para determinar qué eventos o actividades serán vigiladas por el Estado.

Se percibe, por tanto, una ausencia de parámetros reglamentarios y, además, estructuras procesales y administrativas que definan claramente lo que será observado y grabado.

Quinto, existen riesgos con la *selectividad en la grabación de personas participantes de eventos públicos*. En videos examinados de las protestas del 1ro de mayo de 2017 se observan tomas de cámara (mediante el *zoom* del lente) hacia personas en particular por un tiempo sustancial (en lugar de grabar tiros amplios de los eventos). Algunas de estas personas tenían sus rostros tapados, otras no. En una ocasión se hizo un esfuerzo por alcanzar a tomar (y así se establece en la grabación en la que se escucha al agente) la tablilla de un vehículo de motor tipo "pick up", donde estaban unas personas tomando agua y que, aparentemente, eran sujetos de interés para el agente que estaba grabando.

Sexto, se alertó a esta Comisión sobre el riesgo potencial de *uso de compañías privadas por parte de agencias gubernamentales*, fuera de la Policía de Puerto Rico. Aunque no hemos examinado la ocurrencia de esta práctica y esta Comisión no tiene evidencia para concluir que la Policía esté incurriendo en ella, hacemos constar la preocupación de que agencias del gobierno de Puerto Rico establezcan un sistema paralelo de grabación gubernamental llevado a cabo por empresas de seguridad contratadas. De este ser el caso, todas las preocupaciones descritas en este informe serían aplicables a estas instancias; en particular la necesidad de controles al uso de cámaras de vigilancia según la normativa del Tribunal Supremo de Puerto Rico para

esa tecnología. Recordemos que el derecho constitucional a la intimidad es aplicable a actores privados y, en todo caso, se trataría de actores privados realizando funciones tradicionalmente gubernamentales por lo que sería apropiado considerarles como actores estatales responsables de cumplir con todas las exigencias constitucionales.[254]

Algunos de estos asuntos señalados antes, puede que sean atendidos por las nuevas Órdenes Generales. Así por ejemplo, la Orden General 600-610 del 20 de junio de 2018, sobre la Grabación de Eventos Públicos, contiene disposiciones sobre: (a) la grabación íntegra e ininterrumpida de un evento; (b) prohibición de "grabaciones selectivas hacia grupos o personas particulares mientras estos estén en un ejercicio legítimo de su derecho constitucional de expresión"; (c) requisito de adiestramiento y recertificación cada dos años del personal autorizado a grabar; (d) auditorías e inspecciones al azar del material preservado en los servidores; (e) requisitos para la identificación y registro de la evidencia digital previo a su almacenamiento en servidores; (f) requisito para que las grabaciones se mantengan inéditas, entre otras.

Si bien estos cambios representan un adelanto significativo y bienvenido, también es cierto que las preocupaciones antes señaladas se manifestaron en el contexto de una Orden General (del 2014) que a su vez imponía ciertos requisitos. Así, por ejemplo, la edición de videos y la práctica de borrar contenido discrecionalmente, ocurrió ante un mandato reglamentario de preservar los materiales por un periodo de dos años. La adquisición y la intención de uso de varios equipos de vigilancia ("drones"), sin mediar guías claras para su uso y para la protección de derechos

[254] Véase *Empresas Puertorriqueñas de Desarrollo v. HIETEL*, 150 D.P.R. 924 (2000).

constitucionales es particularmente preocupante, especialmente cuando ese equipo tiene la capacidad de introducirse en los recintos más privados de una persona a través de sus ventanas. La ausencia de registros, récords, informes u otros mecanismos de control (necesarios para salvaguardar la integridad del material grabado y evitar su manipulación), ocurrió durante la vigencia de un requisito expreso en la Orden General anterior de que el agente que utilice el quipo de grabación "será responsable de preparar un informe en el que hará constar la fecha, hora, lugar y un resumen de lo grabado". Ante este cuadro, las nuevas directrices—aunque un buen paso— resultan insuficientes ante lo que, a todas luces, es una cultura institucional que no es conducente a la protección de derechos en este contexto.

(d) En cuanto al uso de otra tecnología de información en la Policía de Puerto Rico para fines investigativos

En este renglón concluimos que el Negociado de Tecnología Informática de la Policía de Puerto Rico tiene un rol crucial que cumplir en establecimiento de parámetros reglamentarios para el uso y adquisición de tecnología que tenga el potencial de afectar el disfrute de derechos. Este Negociado tiene como responsabilidad principal la planificación, organización, implantación y mantenimiento de los sistemas computadorizados de información y comunicaciones de la Policía de Puerto Rico y debe someterá recomendaciones sobre las normas y procedimientos relacionados con los sistemas de tecnología y comunicaciones que se implanten.

Considerando los diversos riesgos de potencial mal uso y abuso que cada nueva tecnología puede presentar desde una perspectiva de derechos humanos, resulta evidente para esta Comisión que toda decisión sobre la adquisición de nueva tecnología

debe estar precedida de un análisis de su potencial impacto sobre el disfrute de derechos. Asimismo, es necesario que—por cada tecnología en planes de adquisición—se desarrollen políticas apropiadas y planes de adiestramientos que ayuden a limitar los riesgos de que se afecten los derechos de las personas. En este sentido, el Negociado de Tecnología Informática tiene un rol institucional importante que jugar en la evaluación de estas tecnologías, y en la evaluación del impacto sobre los derechos humanos.

La adquisición de "drones" sin políticas, sin planificiación, sin permisos y sin adiestramiento debe servir como advertencia del impacto previsible sobre los derechos constitucionales de las personas que tendrá el uso futuro de tecnología de vigilancia. Institucionalmente, el Negociado de Tecnología Informática debe cumplir una función de planificación de adquisición tecnología que evite estas posibilidades. No obstante, en el caso de los "drones" específicamente, al parecer se trató de una adquisición que no pasó por esta oficina, lo cual denota una falta de integración entre el Negociado de Tecnología Informática y otros componentes de la Policía.

VIII. Recomendaciones

Tomando en consideración las conclusiones de este informe, la Comisión de Derechos Civiles emite las siguientes recomendaciones.

1. En nuestro sistema de derecho, los funcionarios del Negociado de la Policía de Puerto Rico y del Departamento de Justicia deben abstenerse de incurrir en conductas, prácticas o expresiones que tengan el efecto de disuadir el ejercicio de las

libertades civiles y los derechos a la libertad de expresión y de asociación. En particular, es esencial que las agencias de orden público eviten tomar acción o emitir expresiones críticas contra personas por el sólo hecho de que éstas se manifiesten públicamente (en redes sociales o cualquier otro medio) independientemente de que estas manifestaciones sean cáusticas, agresivas o punzantes. Sólo es constitucionalmente permisible la acción gubernamental en aquellos casos en que las expresiones en cuestión constituyan una "amenaza real", según este concepto es definido constitucionalmente, o una incitación a la violencia que, con alta probabilidad o certeza, vayan a conducir a la violación inminente de la ley. Ausente estas circunstancias extremas, el gobierno no puede crear condiciones de temor en la población de que sus expresiones constitucionalmente protegidas están siendo vigiladas y que posiblemente serán castigadas o referidas a agencias federales.

2. Es necesario que se adiestre a los agentes del orden público respecto a los asuntos cubiertos por este informe, incluyendo:

a. El derecho a la intimidad, a la libertad de asociación y a la libertad de expresión en espacios públicos, particularmente sobre las diferencias entre el derecho a la intimidad bajo los parámetros de la Constitución de los Estados Unidos y bajo la Constitución de Puerto Rico con su amplia interpretación.

b. Las diferencias que existen entre el ordenamiento jurídico federal y el de Puerto Rico con respecto a los derechos de los individuos sobre información personal almacenada por terceros. En particular, es necesario que se adiestre sobre los diversos requisitos constitucionales

que restringen la solicitud de información por el Estado con respecto a esta información.

c. La ilegalidad del monitoreo de las redes sociales de personas o grupos en ausencia de comunicaciones de naturaleza claramente delictiva, distinguiendo lo que podría considerarse conducta expresiva constitucionalmente protegida de la que no lo es.

d. La inconstitucionalidad de realizar monitoreo en las redes sociales sin controles administrativos apropiados o sin que se deje rastro o registro que permita verificar la legalidad de dicho monitoreo.

e. La aplicabilidad de los parámetros constitucionales a los actores de seguridad privada cuando el Estado decide recurrir a esta alternativa por la falta de personal para cubrir eventos públicos.

3. Los funcionarios del Negociado de la Policía de Puerto Rico y del Departamento de Justicia de Puerto Rico deben atenerse a los parámetros más estrictos de nuestra jurisprudencia en cuanto a la solicitud de información personal que está en manos de terceros. Esto exige el cumplimiento con las garantías procesales constitucionalmente requeridas y detalladas en este informe.

4. Corregir o atemperar la Orden General más reciente de la División de Crímenes Cibernéticos del Negociado de la Policía para que se cumpla con los parámetros elaborados por la jurisprudencia del Tribunal Supremo de Puerto Rico, y con los lineamientos elaborados en este informe. Específicamente, esta Orden debe rechazar los parámetros del régimen estatutario federal del *Stored Communcations Act*. Para estar en cumplimiento con la Constitución de Puerto Rico, las solicitudes de

información deben estar precedidas por una orden judicial basada en causa probable de la comisión de un delito o, deben ser sometidas mediante un *subpoena* pero con notificación previa a la persona investigada. Es responsabilidad del Estado proveer a la persona investigada esta notificación, siguiendo los parámetros constitucionales, y no puede descansar en las políticas internas de entidades que almacenan esta información de avisar voluntariamente a las personas.

5. La Orden General 600-610 del 20 de junio de 2018, sobre la "Grabación de Eventos Públicos", debe revisarse para atemperarse a las conclusiones de este informe. En particular, es necesario: (a) establecer controles administrativos más rigurosos que los existentes, que permitan evaluar sistemáticamente el trabajo de la Unidad Técnica de Grabaciones y, por ende, verificar el cumplimiento con las obligaciones constitucionales; (b) establecer claramente prácticas y políticas adicionales para garantizar la integridad del material grabado y almacenado y, de esta forma, evitar su alteración (como, por ejemplo, asignar valores *hash* a archivos digitales que permiten comparar versiones de un archivo almacenado para detectar cambios);[255] (c) establecer criterios claros y procedimientos detallados, de manera que se regule la determinación por parte del Estado en torno a cuáles actividades o eventos públicos serán vigiladas o grabadas; (d) desarrollar prácticas de supervisión más específicas para limitar la selectividad en la grabación de personas o grupos; (e) elaborar procedimientos claros y detallados para borrar y disponer de los videos almacenados

[255] Véase, *United States v. Reddick*, 900 F3d. 636, 637 (5to Cir. 2018) ("Hash values are regularly used to compare the contents of two files against each other. 'If two nonidentical files are inputted into the hash program, the computer will output different results. If the two identical files are inputted, however, the hash function will generate identical output.' Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 541 (2005)".

cuando la reglamentación establecida lo requiere, así como para documentar cuando ello ocurra.

6. Además de las estructuras de supervisión y auditoría interna que puedan establecerse en el Negociado de la Policía de Puerto Rico, es necesario que—de conformidad con recomendaciones emitidas por la American Civil Liberties Union y la Organización Kilómetro 0—"se inicie un proceso de creación de un cuerpo independiente de supervisión ciudadana para la Policía de Puerto Rico. Esta entidad sería una autoridad independiente que investigue la mala conducta policial con acceso a datos, poderes de citación, investigación y auditoría".[256] Toda vez que buena parte de los señalamientos identificados por esta Comisión tienen como base a una cultura institucional deficiente, la mera existencia de políticas mejoradas es insuficiente desde el punto de vista de la protección de derechos. Por esta razón, la "supervisión e investigación de la conducta policiaca no puede reposar en manos de la Policía".[257]

7. Es urgente que la Sección Técnica de Grabaciones cuente con una reglamentación especial que incluya un protocolo para el uso de la tecnología de los "drones", antes de que se utilice la misma. Esta reglamentación debe tomar en cuenta los riesgos particulares que esta tecnología presenta para los derechos de intimidad, asociación y de libertad de expresión.

8. Toda decisión sobre la adquisición de nueva tecnología deber estar precedida de un análisis de su potencial impacto sobre el disfrute de los derechos

---

[256] Luis Manuel Rodríguez y Mari Mari Narváez, *Más Vale Maña que Fuerza: Un análisis critico de los datos de uso de fuerza de la Policía de Puerto Rico contra la ciudadanía*, 4 de diciembre de 2018, página 44, disponible en https://www.kilometro0.org/informes

[257] Id.

constitucionales por la ciudadanía. Esto requerirá que, por cada tecnología que se vaya a adoptar, se desarrollen políticas apropiadas y planes de adiestramiento que ayuden a limitar los riesgos de que se afecten los derechos de las personas. El diseño de estas políticas debe estar informado por procesos de consulta que sean participativos y que tomen en cuenta la opinión de entidades independientes que velen por los derechos humanos como lo es esta Comisión de Derechos Civiles y otras organizaciones de la sociedad civil.

9. Es necesaria la integración y coordinación entre el Negociado de Tecnología Informática con otros componentes de la Policía de Puerto Rico para que el Negociado pueda cumplir su rol en la planificación del uso y de la adquisición de tecnología de forma que cuente con los análisis antes señalados y la reglamentación, protocolos, permisos y adiestramientos requeridos.

10. Vista la seriedad de los hallazgos y conclusiones de este informe, la Comisión de Derchos Civiles considera apremiante que el Negociado de la Policía de Puerto Rico cese y desista de forma inmediata de las prácticas y políticas de vigilancia y monitoreo de actividades de protesta pública que vulneran los derechos de libertad de expresión, asociación e intimidad de las personas.

IX. Notificación

Notifíquese este informe a los querellantes, al Departamento de Seguridad Pública, al Negociado de la Policía de Puerto Rico; al Departamento de Justicia; al Asesor de Cumplimiento Técnico de la Reforma de la Policía, a las tres Ramas Constitucionales del Estado Libre Asociado de Puerto Rico, al Juez Presidente del

Tribunal Federal para el Distrito de Puerto Rico, al Departamento de Justicia de los Estados Unidos, a la Unión Americana de Libertades Civiles (ACLU, por sus siglas en inglés), Kilómetro 0, a los medios de comunicación del país, a las bibliotecas de las escuelas de derecho en Puerto Rico y a la Biblioteca del Tribunal Supremo de Puerto Rico.

En San Juan, Puerto Rico hoy 24 de abril de 2019.

Lcda. Georgina Candal Segurola
Presidenta

Dra. Esther Vicente
Vicepresidenta

Dr. Hiram Meléndez Juarbe
Comisionado

Lcda. Patricia Otón Olivieri
Comisionada