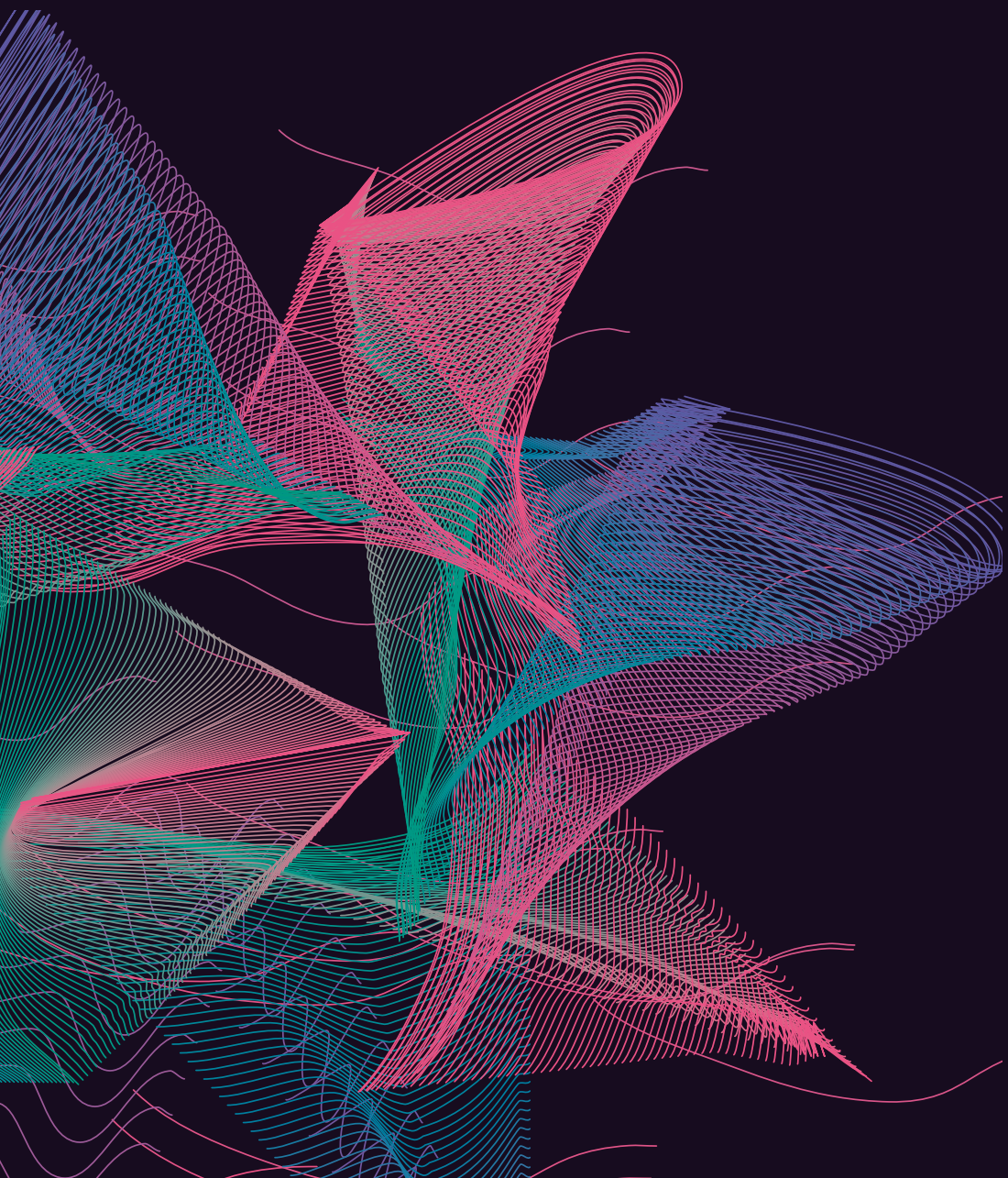
POR LA DEFENSA DE LOS DATOS PERSONALES EN PARAGUAY

Compendio de ensayos de la Clínica 2022

«Derecho a la privacidad y datos personales»



Tecnología & Derechos Humanos

TEDIC

POR LA DEFENSA DE LOS DATOS PERSONALES EN PARAGUAY

Compendio de ensayos de la Clínica 2022

«Derecho a la privacidad y datos personales»

Tecnología & Derechos Humanos

La Clínica Jurídica 2022 fue realizada por la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Asunción conjuntamente con TEDIC, en esfuerzo cooperativo sobre la base de un convenio de ambas instituciones e INDELA , con el apoyo del Programa Estado de Derecho y Cultura de la Integridad, impulsado por el Instituto Desarrollo con apoyo de USAID/Paraguay.

El contenido del presente documento es responsabilidad de los autores y no refleja necesariamente los puntos de vista o las posiciones de la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Asunción, Instituto Desarrollo, TEDIC, INDELA, ni de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) o el Gobierno de los Estados Unidos.

ORGANIZAN

APOYAN

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

POR LA DEFENSA DE LOS DATOS PERSONALES EN PARAGUAY

COMPENDIO DE ENSAYOS DE LA CLÍNICA 2022 «DERECHO A LA PRIVACIDAD Y DATOS PERSONALES»

AGOSTO 2023

COORDINACIÓN
Dra. María Mercedes Buongermini, Facultad de Derecho y Ciencias Sociales UNA
Abg. Maricarmen Sequera, TEDIC
Abg. Leonardo Gómez Berniga, TEDIC
Abg. Cira Montserrat Ávalos, Facultad de Derecho y Ciencias Sociales UNA

AUTORES/AS
Hugo Mendieta Cuevas
Sergio Bestard
Susana Florentín Godoy
Sofía Rattazzi
Juan D. Romero Sanabria
Alfredo Daniel Barrios Duarte
Álvaro Penayo
Giovanni Beconi
Agustina Maria Rodríguez Alcalá Castagnino

DISEÑO Y DIAGRAMACIÓN
Horacio Oteiza

SUMARIO

SOBRE LA CLÍNICA JURÍDICA

La segunda edición de la Clínica Jurídica de Derechos Digitales denominada “Derecho a la privacidad y datos personales”, organizada en conjunto por TEDIC y la Facultad de Derecho Ciencias Sociales de la Universidad Nacional de Asunción, buscó visibilizar y generar una discusión informada sobre la necesidad de contar con un marco jurídico integral de protección de datos personales en Paraguay.

El desarrollo de la misma estuvo a cargo de las abogadas Prof. María Mercedes Buongermini, Maricarmen Sequera, Prof. Cira Montserrat Avalos y el abogado Leonardo Gómez Berniga.

Desde su primera edición, la clínica tiene por objeto promover los derechos humanos en entornos digitales, impulsar la perspectiva de derechos humanos en implementación de tecnología y la práctica jurídica en esta área del derecho[1]. Tras la evaluación de postulaciones recibidas, se seleccionaron diez alumnos y alumnas que formaron parte de esta iniciativa, implementada como actividad de extensión universitaria dentro de la carrera de Derecho. La propuesta estuvo dirigida a estudiantes que hubieran finalizado el quinto semestre, con base en conocimientos sobre derechos humanos.

El desarrollo formal de la actividad se hizo desde octubre a diciembre del 2022, y las tutorías se extendieron hasta el primer semestre del 2023.

Entre las actividades desarrolladas se contaron talleres con clases magistrales sobre datos personales y derecho a la privacidad, taller intensivo sobre escritura académica y gestión bibliográfica, y una tutoría dedicada para la identificación de temas de datos personales y expedientes judiciales en proceso o finiquitados; por último se tuvo un espacio dedicado a la elaboración de los trabajos finales, a continuación presentados.

Paraguay aún no cuenta con una Ley Integral de Protección de datos personales, lo que lo ubica —junto con Bolivia— entre los únicos países de la región donde hay un vacío legal que afecta derechos fundamentales de la población. En la actualidad se encuentra en Cámara de Diputados un proyecto de ley impulsado por la Coalición de Datos Personales en Paraguay —de la cual es integrante TEDIC—, presentado por actores políticos de diversos partidos políticos y con un dedicado acompañamiento de la Comisión de Ciencia y Tecnología del órgano legislativo.

1 https://www.tedic.org/clinica-juridica-de-derechos-digitales/

PRÓLOGO: TUS DATOS, TUS DERECHOS

por Leonardo Gómez Berniga, TEDIC[2]

En TEDIC reconocemos la importancia de fomentar espacios de diálogo especializados y críticos que contribuyan a la creación de conciencia y conocimiento en torno al derecho a la privacidad y datos personales. ¡Es urgente! Paraguay necesita adaptarse a los nuevos estándares que ponen la protección de la privacidad en el centro de la expansión del acceso a servicios, conocimientos y el desarrollo de tecnología en el sector público y privado.

En un contexto global donde enfrentamos desafíos complejos en términos de derechos digitales, nos encontramos con la creciente presencia de modelos de aprendizaje profundo o inteligencia artificial, flujos transfronterizos de datos y la manipulación de nuestros datos por grandes empresas con políticas de transparencia cuestionables. Todo esto, junto a las tensiones de soberanía nacional, enfatiza la necesidad de una legislación clara que nos proteja.

Cada acción que tomamos, lo que vemos, consumimos, e incluso lo que somos, deja huellas que se convierten en datos personales. Entonces surge una pregunta crucial: ¿a quién confío mis datos? A menudo, estos datos pueden revelar más sobre nosotros que lo que decimos verbalmente.

Este cuestionamiento ha desencadenado debates importantes en todo el mundo, cada vez más relevantes. En las últimas cuatro décadas, los países han establecido marcos legales sólidos no solo para proteger la intimidad, sino también para defender la autonomía del individuo en el control de sus datos. Tienes el derecho de apelar, solicitar información y prevenir el abuso de tus datos tanto por el Estado como por las empresas.

Desde su fundación en 2012, TEDIC ha estado promoviendo una Ley Integral de Protección de Datos Personales. Aunque han logrado reunir a varios actores en esta causa y han formado la Coalición de Datos Personales, las respuestas actuales son insuficientes frente a la urgencia de la situación. Paraguay, junto con Bolivia, son los únicos países de la región que aún no cuentan con una ley nacional que proteja a sus ciudadanos de los abusos en materia de datos personales, aunque a nivel subnacional recientemente el país vecino tomó la delantera.

Esta situación debe abordarse desde una perspectiva de derechos humanos, especialmente en un mundo en el que las tecnologías “deshumanizantes”, el espionaje y el uso indebido de datos personales son una realidad constante. Esperamos que la ley, actualmente en la Cámara de Diputados, avance hasta el Senado y su existencia se convierta en un acto de justicia y consolidación del Estado de Derecho que frente a sus dificultades y deudas encuentra en actores políticos, la sociedad civil organizada y la academia, aliados fundamentales.

---

2 Coordinador de proyectos sobre Tecnopolítica y Democracia en TEDIC. Abogado por la Universidad Nacional de Asunción (UNA) y candidato a magíster en Derechos Humanos y Democratización en América Latina y el Caribe por la UNSAM (Argentina); Especializado en didáctica de la Educación Superior (INAES) y comunicador. Con más de 10 años de experiencia de trabajo en organizaciones de la sociedad civil locales e internacionales. Realiza investigaciones en asuntos electorales, social media analytics, tecnopolítica, democracia y políticas públicas. leonardo@tedic.org

La Coalición de Datos Personales de Paraguay y los legisladores que respaldan esta iniciativa han trabajado arduamente y, al cierre de este documento, el proyecto de ley presentado en 2021 espera ser discutido ante el pleno de la Cámara de Diputados antes de fin de año tras tres postergaciones en el orden del día. Esta ley, que ha sido revisada por más de 30 informes de instituciones públicas y privadas, representa un hito importante en nuestra lucha por la privacidad.

Los legisladores tienen la oportunidad de defender a la población de los abusos diarios a la privacidad en Paraguay. No queremos mensajes no solicitados, llamadas comerciales intrusivas ni manipulación política basada en datos sensibles. ¡El momento de la justicia es ahora! Apoyemos una ley de protección de datos personales ya.

Estoy convencido que desde la tarea de coordinación de la Clínica en su segunda edición, con el valioso concurso de la Dirección de Investigación de la Facultad de Derecho y el exhaustivo esfuerzo depositado en cada uno de los y las estudiantes que nos honran con sus ensayos, esperamos que las personas lectoras encuentren en las siguientes líneas nuevas preguntas, nuevos planteamientos y sobre todo, convicción en la defensa de los derechos humanos en su intersección con la tecnología.

La identificación de temas sumamente relevantes cruzados con la realidad nacional caracteriza cada uno de los ensayos a continuación disponibles. El primero, de Beconi y Rodríguez Alcalá, evidencia a partir de un estudio de caso los desafíos en materia de protección de datos recopilados en el ámbito crediticio, la necesidad de contar con una mejor armonización en la materia, donde factores cómo la innovación, derechos del consumidor y la globalización obligan a que exista una autoridad de aplicación especializada, cual es uno de los objetos centrales para garantizar la eficacia en la implementación de cualquier normativa en la materia.

El segundo ensayo, de Rattazzi y Romero, toca otro tema central ante la emergencia del capitalismo de plataformas, de la “uberización” del consumo informacional y la confluencia entre protección de datos, derecho a la intimidad, derechos intelectuales y violencia de género. En palabras breves y concisas, e invitando a disparar más preguntas, nos acerca a pensar cómo la plataforma Onlyfans existe y merece una conversación desde el derecho, invitando a salir de una lectura superficial a una caracterización de posibles víctimas de derechos en el espacio digital.

¿Quién vigila al vigilante? ¿Qué tan “inteligente” es hipervigilar a la población en las ciudades? La tecnología implementada recientemente en el país y en la región, ¿está realmente al servicio de la población o emerge como una amenaza? Con un análisis provocativo y un ensayo rico en referencias, Mendieta, Bestard y Florentin alertan sobre cómo la tecnología, haciendo uso abusivo de datos, puede afectar libertades fundamentales; cómo la libertad de asociación, reunión, expresión y pensamiento, violando la intimidad, pueden llegar a profundizar la marginación social de sectores históricamente excluidos y resquebrajar pilares de la democracia, como, por ejemplo, la presunción de inocencia.

Por último, con precisión legal y un análisis oportuno, Penayo y Barrios, realizan un análisis legal del recurso de amparo presentado por TEDIC en el 2018 ante la Corte Suprema de Justicia, ante una negación de acceso a la información pública sobre compra de tecnología de cámaras de videovigilancia con reconocimiento facial en Paraguay por parte del Ministerio del Interior. El caso ha superado la primera y segunda instancia en lo legal, y la solicitud ha sido denegada. Actualmente se encuentra en la Sala Constitucional, tras la presentación de una acción de inconstitucional.

El análisis fortalece, desde una mirada local y punto por punto, los motivos por los cuales corresponde la procedencia del amparo, considerando que es un caso de interés difuso, que no existe otra figura legal por la cual se pueda incoar la acción peticionada y, además, puntualizando que se han agotado todas las vías administrativas posibles para efectivizar el cumplimiento del derecho constitucional.

Este oportuno análisis se alinea con posicionamientos brindados en el caso por organizaciones internacionales, como Access Now y Artículo 19, quienes se presentaron a la Corte en carácter de amicus curiae, cómo a la exigencia reciente que viene haciendo TEDIC, con apoyo de la Coalición por la legalidad, impulsada por Fundación CIRD.

LA FALTA DE AVANCES LEGALES EN MATERIA DE PROTECCIÓN DE DATOS VULNERA NUESTRA PRIVACIDAD

Giovanni Beconi & Agustina Maria Rodríguez Alcalá Castagnino

LA FALTA DE AVANCES LEGALES EN MATERIA DE PROTECCIÓN DE DATOS VULNERA NUESTRA PRIVACIDAD

— por Giovanni Beconi[3] & Agustina Maria Rodríguez Alcala Castagnino[4]

¿Cuántas veces al día realizamos operaciones en las que intermedian plataformas digitales?… Probablemente en muchas ocasiones.

En Paraguay, al igual que en la mayor parte del mundo, resulta innegable el avance en la comunicación y comercio por los medios digitales. Por tal razón, existe una enorme cantidad de datos personales que se recopilan constantemente por parte de actores públicos y privados, y para diversos fines. En este sentido nuestra legislación e instituciones no se encuentran preparadas para poder sobrellevar las implicancias de lo mencionado debido a una serie de razones.

Globalización del mercado actual

La globalización ha transformado al mundo humano en un solo mercado. Las transacciones comerciales se realizan por minutos y segundos; las empresas transnacionales aumentan su productividad mediante la tecnología aplicada a la producción, reduciendo costos, tiempo y aumentando la producción, para adecuarse a las necesidades actuales del mercado.

La masificación de avances en los negocios electrónicos es un fenómeno que ha transformado la sociedad, resignificando una multitud de procesos jurídicos. Esto ha dado nacimiento a un sistema de contratación masiva por un mecanismo de repetición de las operaciones. Tal situación ha impactado en una clara disminución de la autonomía de la voluntad, aceptando obligaciones con un simple gesto, como un click o un toque a la pantalla del *smartphone.*

¿Cuál es la importancia de los datos personales?

El Estado Paraguayo tiene un déficit en materia de protección de datos personales, dejando potencialmente en situación de vulnerabilidad a los datos de todos los usuarios de plataformas digitales. Ello, debido a la inexistencia de una ley integral de protección de datos personales.

Esto contrasta con que, actualmente, se encuentra vigente la Ley 6534 “De Protección de Datos Personales Crediticios”. La misma es limitada en su alcance y posee lagunas legales en cuanto a temas como la reparación ante casos de abuso. Concretamente, esta ley no prevé mecanismos de reparación efectivos y hacen que la carga económica de buscar algún tipo de reparación ante el mal uso de datos personales recaiga sobre las espaldas de la ciudadanía.

Riesgos y oportunidades en el caso de las Fintech

Cuando cada uno de nosotros suscribe un contrato de prestación de servicios mediante una intermediación tecnológica, es muy probable que una serie de datos sean requeridos sobre nuestra persona. Estos pueden ir desde lo básico, como nuestra identidad, hasta datos tan complejos como los datos de salud.

---

3 Estudiante de la carrera de derecho en la Universidad Nacional de Asuncion. Estudio Beconi. gb@eb.com.py

4 Estudiante de la carrera de Derecho en la Universidad Nacional de Asunción (UNA). Poder Judicial. agustinamariarodriguezalcalaca@gmail.com

La ausencia de una ley integral de protección de datos personales y de políticas de protección de datos personales posibilita la ocurrencia de diversas situaciones en las cuales queda abierta la posibilidad de recopilar datos no necesariamente referentes a la actividad comercial realizada. Esto es, se recopilan más datos de los necesarios para la transacción puntual. Es importante aclarar que en materia de protección de datos personales es clave definir el propósito y la necesidad de recopilar ciertos tipos de datos, así como los límites en el uso de los mismos.

Un caso práctico: UENO

Una empresa que ha estado posicionándose en el mercado el último año es la financiera UENO[5]. Esta *fintech*[6] incorporó a nuestro país un nuevo sistema de descuentos: El usuario, al realizar transacciones en ciertos negocios, recibe un beneficio automático, obteniendo la devolución de un porcentaje del monto abonado, ya sea del 30 hasta el 50 %. Esto capturó masivamente el interés de los consumidores, gracias a una fuerte campaña de marketing que logró atraer a un gran porcentaje de la ciudadanía. A través de esto la nueva plataforma accedió y obtuvo información personal de sus usuarios, y puso de relieve la escasez de políticas de privacidad brindadas a los mismos. Es importante destacar que la mayor parte de los usuarios son jóvenes, cosa preocupante ya que los mismos con un simple click proceden a dar mucha información personal.

¿Cómo puede mejorar UENO sus políticas de protección de datos personales?

¿Qué tipos de datos trataremos?

Financiera ueno S.A.E.C.A. podrá tratar:

- Tus datos generales.
- Tu información básica: como nombre completo, edad, edad más probable, situación sentimental, dirección de residencia y número de contacto, dirección de residencia y número de contacto más probable, dirección del lugar de la actividad económica, dirección más probable del lugar de la actividad económica, fecha de nacimiento, correo electrónico, correo electrónico más probable, datos en el registro civil, resolución de expedición del documento de identidad, fecha de expiración de documento de identidad (si aplica), tipo de documento de identidad y demás datos en tu documento de identidad, datos en otros documentos públicos, estado de tu registro civil y de tu documento de identidad, residencia fiscal u obligación de pagar tributos en otros países, si eres una persona con exposición política o pública, y otros datos demográficos.
- Tu información financiera: como estatus de empleado / independiente o pensionado, actividad económica como tal, ingresos, gastos, activos, pasivos, potenciales pasivos (por ejemplo, si eres codeudor o fiador, o si tienes aperturas de crédito o cupos de endeudamiento), patrimonio, cotizaciones a seguridad social, estado de obligaciones, flujos de efectivo, cheques devueltos, sobregiros, extractos, seguros, fianzas u otros respaldos, o indicadores y estimaciones sobre los anteriores.

Más adelante podrás conocer para qué vamos a tratar tus datos y aplicar estos ejemplos a un caso concreto. Continúa leyendo, nos hemos esforzado para que conozcas lo que otros todavía no te han explicado bien.

Aquéllos con quienes tienes o has tenido relaciones laborales, comerciales, financieras o de seguridad social, junto con el tipo y estado de dichas relaciones, según se encuentre dicha información en centrales de riesgo o de información.

- Tu georreferenciación o geolocalización específica.
- Información sobre tus preferencias de consumo, objetivos y tolerancia a riesgos, no solamente con referencia a nuestros productos o servicios, sino a productos o servicios de terceros.
- Tu rastro digital en redes sociales, comercios, buscadores y otras páginas web.
- Otra información que nos proporciones, por ejemplo, en las encuestas, concursos, campañas y lanzamientos de nuevos productos y servicios en los que decidas participar directamente a través de nuestros canales oficiales o a través de terceros (por ejemplo, a través de tus redes sociales), o en otras interacciones con nosotros.

5 https://www.ueno.com.py/

6 BBVA. FINTECH: Se podría definir como la suma de 'financial' y 'technology', un movimiento donde muchas pequeñas empresas quieren cambiar la forma en la que entendemos los servicios financieros utilizando la tecnología.

- Información sobre tu calidad de persona expuesta públicamente y sobre tus antecedentes (judiciales, administrativos o de otro tipo), así como sobre tus relaciones con personas con calidad de persona expuesta públicamente o con tales antecedentes.
- Tus datos sensibles.
- Tu género.
- Tu origen racial o étnico.
- Otros datos que nos suministres y que lleguen a ser catalogados como datos sensibles.

Importante: En muchos casos no buscamos obtener estos datos, pero puede que los lleguemos a tratar indirectamente. Evitaremos que con tus datos sensibles se genere discriminación (indebida o negativa). Las normas te protegen.

Creemos que la Financiera UENO debería tomar la iniciativa y adoptar una política empresarial que priorice la protección de los datos personales. Así, la misma podrá diferenciarse de sus competidoras, y no solo destacarse por sus descuentos, sino también por ocuparse de la protección de los datos personales de sus personas usuarias. Es llamativo que esta plataforma solo dé a sus usuarios el aviso de privacidad consensuado por el consumidor, habilitando a que la entidad recopile **datos sensibles (sin protección alguna)**, los cuales pueden ser posteriormente compartidos con otros intermediarios del mismo grupo empresarial, ya que en el derecho privado, lo que no está prohibido está permitido. (Aviso de privacidad UENO, 2022).

Por otra parte, si bien es celebratorio que en esas políticas se menciona una garantía de no discriminación con base en la recolección de datos sensibles, no se especifica qué medidas concretas serán tomadas por UENO para evitar tales situaciones o hechos.

Es importante que UENO establezca claramente cuáles son los tipos de datos personales que son efectivamente necesarios para una correcta prestación de servicios financieros digitales y cuáles no.

Los datos de carácter sensible son particularmente importantes de resguardar, ya que permiten hacer inferencias respecto de cuestiones sensibles, como orientación sexual o política. Esto, en determinados contextos, puede terminar en situaciones de discriminación a las personas. Tal como establece la propia ley de datos personales crediticios, los datos personales sensibles son *"Aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física".*

El aspecto procesal de las políticas de datos

Al ser la recopilación de datos algo tan amplio que abarca a personas de diversos orígenes, edades, estratos económicos, nivel educativo etc., resulta muy importante que su información personal sea de fácil acceso para las mismas. En este sentido, los recopiladores de datos[7] son poco claros en cuanto a sus políticas de acceso de datos por el titular, muchas veces inexistente.

Cuando comparamos nuestra casi nula protección legal con, por ejemplo, las normas del Reino Unido, vemos cómo éste claramente establece con amplitud los derechos del titular en materia de protección de datos personales, además de los plazos de contestación del encargado. Eso resulta de suma importancia, ya que de esta manera se garantiza el conocimiento preciso de las opciones que el titular tiene en cuanto al manejo de su propia información. (2018 - Data Protection Act, s. f., art. 45)

7 Aquellas instituciones públicas o privadas que recolectan datos personales en distintas maneras y escalas.

La inexistencia de esta delimitación condena a cualquier persona que decida ejercer su derecho a la información a una nebulosa jurídica en la cual potencialmente podría darse algún tipo de abuso por parte de la entidad recopiladora.

Las instituciones designadas para regular el tratamiento de datos actualmente no se especializan en la materia

La *Ley 6534/20 "De Protección de Datos Personales Crediticios"* establece dos instituciones encargadas de regular el cumplimiento de esta norma; éstas son el Banco Central del Paraguay (BCP) y la Secretaría de Defensa del Consumidor y el Usuario (SEDECO)

Analizando la resolución reglamentaria de esta ley, efectuada por la Secretaría de Defensa del Consumidor y el Usuario (SEDECO), encontramos que todo el proceso de fiscalización de los proveedores recae sobre cuatro direcciones:

- La Dirección Nacional de Procedimientos
- La Dirección Nacional de Fiscalización
- La Dirección Nacional de Asuntos Jurídicos
- La Dirección Nacional de Administración y Finanzas

Está por verse el nivel de efectividad real de estas direcciones para garantizar el derecho de los titulares de los datos personales. Sin embargo, es importante destacar que el derecho a la protección de los datos personales no persigue necesariamente un fin meramente económico, sino también garantizar la decisión del titular sobre qué desea y qué no desea que se sepa de sí mismo.

Más que nunca es necesaria una ley general de protección de datos personales

Es fácil darnos cuenta del grado de exposición al cual las personas se encuentran sujetas en la actual sociedad de la información. En ese sentido, no solamente nuestras instituciones no disponen de la capacidad suficiente para regular en su totalidad el tráfico de información, sino también es inexistente la regulación de aquellos datos que van más allá de la actividad crediticia.

Lo común resulta ser la ausencia de protocolos de tratamiento de datos personales. Esto nos coloca muy por debajo del estándar internacional y expone a los usuarios a todo tipo de riesgos, como ataques informáticos, entre otros. (Fulchi, Sequera, 2018).

Hasta entonces, la mejor metáfora que podemos hallar de nuestra situación es la de un barco a la deriva.

Referencias

1. 2018—*Data Protection Act 2018.pdf.* (s. f.).
2. *Aviso de privacidad UENO.* (2022).
3. Barberán, P. (s. f.). *ASPECTOS JURÍDICOS DE LAS APLICACIONES MÓVILES (APPS).*
4. *Carta de los Derechos Fundamentales de la Unión Europea.* (s. f.). 17.
5. Indacochea Jauregui, J. M. (2020). La jurisprudencia andina y europea en materia de protección del software, las aplicaciones móviles y los videojuegos. *Revista Tribuna Internacional, 9*(18), 97. https://doi.org/10.5354/0719-482X.2020.59455
6. Fulchi, Sequera (2018) *La Protección de Datos Personales en el Sector Privado de Paraguay.* (s. f.)
7. Torres Kirmser, J. R., Ríos Avalos, B., Beconi Ortiz, F. A., & Rodríguez González, A. J. (2018). *El derecho comercial y su globalización*. Intercontinental Editora.

ONLYFANS EN PARAGUAY: VULNERACIÓN DE LA PRIVACIDAD Y DESAFÍOS LEGALES

Sofía Rattazzi & Juan D. Romero Sanabria

ONLYFANS EN PARAGUAY: VULNERACIÓN DE LA PRIVACIDAD Y DESAFÍOS LEGALES

— por Sofía Rattazzi[8] & Juan D. Romero Sanabria[9]

En la actualidad, gran parte de las actividades comunes de las personas se realizan a través de medios digitales. Se pueden suscribir contratos, realizar transacciones, trabajar online, generar contenido, entre otros. Tal es el caso de Onlyfans, una plataforma digital en la cual se pueden ver reflejadas varias de las actividades que se han mencionado previamente.

Onlyfans funciona como una plataforma en línea que permite a las personas creadoras de contenido monetizar su material, con sus respectivos suscriptores ("fans"). La plataforma actúa como intermediaria entre ambas partes, cobrando un porcentaje por el acceso al contenido.

Los *fans* son aquellos individuos que, mediante el pago de una suscripción mensual, obtienen acceso a fotografías y videos exclusivos ("contenido"). Esta modalidad de producción de contenido digital se ha convertido en una forma curiosa e interesante de generar ingresos.

En Onlyfans la elección del tipo de contenido está a cargo de cada creador; sin embargo, la categoría más rentable se ha vuelto el contenido erótico y sexual. El escenario económico de la pandemia por el COVID-19 propició que la misma sea utilizada en varios países, entre ellos Paraguay, convirtiéndose en un medio generador de ingresos. A través de su creatividad, los creadores de contenido producen material interesante para sus *fans*.

El avance tecnológico en las relaciones humanas ha llevado a un aumento en el uso de medios digitales para generar ingresos económicos. Sin embargo, esta tendencia también ha dado lugar a situaciones en las que los derechos de las personas pueden ser vulnerados.

La viralización de imágenes de Onlyfans en otras plataformas y redes sociales es una realidad que afecta a los creadores de contenido. Esto ocurre cuando los *fans* que han adquirido el acceso al contenido exclusivo lo comparten en sitios o plataformas ajenas, sin consentimiento de la persona creadora del contenido. La protección del contenido digital y los derechos de autor son aspectos especialmente importantes en este contexto, dada la facilidad con que el contenido puede ser copiado y distribuido en línea.

> "Las personas que ven tu contenido pueden compartirlo con otros sin ningún problema. Es fácil tomar una captura de pantalla o descargar el material con aplicaciones alternas. Por lo que es posible obtener un suscriptor que sí compre tu contenido, pero después lo pueda revender en páginas de pornografía." (Fajardo, 2021)

---

8 Abogada por la Universidad Nacional de Asunción. Estudiante de la Especialización en Gobernabilidad, Gerencia Política y Gestión Pública en la Universidad Columbia y la George Washington University. Miembro del Consultorio Jurídico de la Facultad de Derecho de la UNA. sofiarattazzi13@gmail.com

9 Abogado por la Universidad Nacional de Asunción. Mediador Universitario por el Centro de Estudios Judiciales. Miembro del Consultorio Jurídico y colaborador en distintos proyectos de investigación y de extensión universitaria en la Facultad de Derecho y Ciencias Sociales de la UNA. juanromeropy99@gmail.com

La difusión no consentida del contenido compartido en Onlyfans transgrede los derechos sexuales y reproductivos, el derecho a la intimidad y causa un daño patrimonial a la víctima. En ese sentido, el art. 110 de la C.N. menciona: “De los derechos de autor y de propiedad intelectual: Todo autor, inventor, productor o comerciante gozará de la propiedad exclusiva de su obra, invención, marca o nombre comercial, con arreglo a la ley”. Como obras de contenido artístico, las fotografías y videos colgados en el sitio Onlyfans se encuentran sujetos a derechos de autor. Estos derechos nacen en el momento en que la obra es creada, en este caso, una vez que la fotografía haya sido pensada y posteriormente tomada por la persona en cuestión (Grupo Atico34, 2021).

En su mayoría, las víctimas de este tipo de transgresiones son mujeres. A pesar de que los creadores de contenido son de diversas orientaciones sexuales, la cosificación del cuerpo femenino se ha normalizado en los medios de comunicación y en las redes sociales. Esta situación deja a las creadoras de contenido más expuestas a la violencia digital y a la vulnerabilidad de sus datos personales.

En estos casos, es crucial que la justicia y las leyes ofrezcan una respuesta rápida y eficaz a la persona afectada. No obstante, las normas existentes buscan únicamente salvaguardar bienes jurídicos como el honor o la reputación. En nuestro país no existe actualmente un marco jurídico que proteja el contenido explícito que se publica en la plataforma Onlyfans, lo que deja a las personas que crean este tipo de contenido en una situación de vulnerabilidad.

En efecto, actualmente las normas existentes se enfocan en proteger bienes jurídicos como el honor o la reputación, pero no hay un marco jurídico que proteja el contenido explícito publicado en estas plataformas. Esta situación deja a las personas creadoras de este tipo de contenido en una posición vulnerable.

Por ello resulta fundamental que la justicia y las leyes proporcionen una respuesta rápida y efectiva a las personas afectadas por la difusión no autorizada de contenido explícito en plataformas como Onlyfans. El Estado debe legislar con miras a la prevención y sanción de conductas que vulneren los derechos de las personas, adaptándose a la realidad digital actual.

En definitiva, es fundamental reconocer y proteger los derechos de autor, los derechos sexuales y reproductivos, y el derecho a la intimidad en la era digital, a fin de garantizar una convivencia responsable y segura en los medios digitales.

Referencias

1. Fajardo, A. (2021, agosto 20). Only Fans, ¿una discusión moral o económica? Memorias de Nómada. https://www.memoriasdenomada.com/only-fans-discusion-moral-o-economica/ https://www.memoriasdenomada.com/only-fans-discusion-moral-o-economica/

2. Grupo Atico34. (2021, octubre 5). Los derechos de imagen en la fotografía. Grupo Atico34. https://protecciondatos-lopd.com/empresas/derechos-imagen-fotografia/

WATCHMEN TECNOLÓGICO: EL PELIGRO DE LAS *SMART CITIES* POLICIALES

Hugo Mendieta Cuevas, Sergio Bestard & Susana Florentín Godoy

WATCHMEN TECNOLÓGICO: EL PELIGRO DE LAS SMART CITIES POLICIALES

— por Hugo Mendieta Cuevas[10], Sergio Bestard[11] & Susana Florentín Godoy[12]

At midnight all the agents and the superhuman crew

Come out and round up everyone who knows more than they do.[13]

Bob Dylan, *Desolation Row.*

Este artículo examina las implicaciones de la ejecución de sistemas de vigilancia masiva dentro de las *smart cities*[14]. A nivel mundial existe una tendencia creciente hacia la utilización de tecnologías de vigilancia en el marco de las ciudades inteligentes, y esta inclusión tecnológica presenta riesgos insalvables con respecto a los Derechos Humanos. El artículo aboga por la supresión y prohibición de cualquier programa de vigilancia a escala masiva que pueda plantearse con algún proyecto similar al que están llevando adelante en la región[15] con la *smart city*.

Las *smart cities* representan un nuevo enfoque en las ciudades y, por ende, también generan un nuevo paradigma en torno a los derechos humanos, la aplicación de las tecnologías, la vigilancia y sus límites. El concepto de *smart city*[16] (ciudad inteligente) no puede encerrarse en una sola dimensión, ya que se compone de varias aristas y direcciones. En algunos aspectos tiene que ver con la planificación urbana de una ciudad, en otros con las telecomunicaciones, pero aunque tengan diferentes componentes poseen un punto en común, que es imprescindible para la cosmovisión que se plantea con este tipo de ciudades: la vigilancia.

El proyecto de *smart city* se implementa sobre la base de la vigilancia y la recolección de datos de las personas que habitan y circulan por la ciudad. Esta información, además de permitir desarrollar políticas públicas eficaces (que es como justifican su aplicación), es deseada por las empresas que trabajan con big data[17] y utilizan estos datos para fines comerciales, incluso violentando la privacidad

---

10 Estudiante de derecho en la Universidad Nacional de Asunción. Colaborador en proyectos de extensión universitaria en el Instituto Desarrollo. Colaborador en el segmento de cultura del periódico digital «Adelante!». hugommcuevas@gmail.com

11 Estudiante de la carrera de Derecho en la Universidad Nacional de Asunción (UNA). Actualmente trabajando en la Corte Suprema de Justicia. sergibestard@gmail.com

12 Estudiante de cuarto año de la carrera de Derecho en la Universidad Nacional de Asunción. Cuenta con una especialización en Didáctica Universitaria por la Facultad de Filosofía de la misma universidad. Licenciada en Ciencias Políticas por la Escuela de Ciencias Sociales y Políticas de la UNA. luxantrip@gmail.com

13 Traducción: A medianoche, todos los agentes y la tripulación sobrehumana salen y reúnen a todos los que saben más que ellos.

14 A lo largo del texto se utilizan indistintamente los términos “smart city”, “smart cities”, “ciudad inteligente” y “ciudades inteligentes”.

15 Mc Manus, A., Noguera, A., & Smart, S. (2022)

16 “En la actualidad, el término más usado para referirse a la implementación de tecnologías digitales, –como las tecnologías de la información, el Internet de las cosas (IoT, por su sigla en inglés) o las tecnologías de blockchain– para transformar los espacios y la experiencia urbana, es el de smart city.” (Mc Manus et al., 2022)

17 Conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios.

de la gente. Es necesario discutir esta evolución tecnológica en el marco de los derechos humanos y los principios internacionales en materia de vigilancia. La ciudad inteligente, tal como está planteada, con su piedra angular en la vigilancia (tanto policial como comercial) implica un potencial de violación de derechos fundamentales y constitucionales.

Sin un marco legal concreto y específico, incluyendo la seguridad del tratamiento de los datos, la posibilidad de aplicar los diversos programas de vigilancia debe descartarse por completo; la tecnología no es el problema, sino el contexto en que ella podría aplicarse. En Paraguay no existe aún ni siquiera una ley de protección de datos personales, y es por ello que no están dadas las condiciones para asegurar el respeto por los derechos de las personas en la aplicación de las dinámicas "inteligentes" que requieren los programas integrales de vigilancia: circuito cerrado de televisión (CCTV), reconocimiento facial, geolocalización, drones, etc.

La vigilancia que sirve de base para la ciudad inteligente debe, asimismo, plantearse tomando en cuenta el debate que actualmente se tiene sobre la expectativa de privacidad en espacios públicos. Si bien la Corte Interamericana de Derechos Humanos (CIDH) reconoce los peligros que conllevan los sistemas de vigilancia masiva, y que su aplicación debe ceñirse estrictamente a los principios de legalidad, proporcionalidad y necesidad, esta recomendación es insuficiente para prevenir violaciones sobre la privacidad y otros derechos fundamentales a nivel local de laca país. La policía de Paraguay tiene antecedentes reprobables en lo que se refiere al cumplimiento del principio de proporcionalidad; las evidencias en Francia (Offner, 2018) muestran que los vicios anteriores solamente se acrecientan con el "solucionismo tecnológico"[18], narrativa que es presentada en el marco de las políticas neoliberales desde Silicon Valley hasta Santiago.

Ciertamente el mundo es cada vez más digital; tanto, que los datos de las personas se procesan a una escala mucho mayor. Desde las comunicaciones por redes sociales hasta las búsquedas en internet, todas las actividades humanas en espacios y entornos digitales generan el interés de las empresas y, por obvias razones, en los estados. La privacidad de las diversas acciones está siendo reducida a lo mínimo posible bajo la excusa de una promesa: la solución tecnológica para asegurar la democracia.

La *smart city* fue presentada al mundo como un proyecto que solucionaría los problemas urbanos a comienzos del siglo XXI, en el marco de un proyecto político que pretendió solventar tales problemas con la tecnología, pero sin tratar las cuestiones de fondo que los generaban (inseguridad, tráfico, sostenibilidad, etc.), y esto implicó el sacrificio de la privacidad en favor de la vigilancia.

El interés estatal en Paraguay por la aplicación de la ciudad inteligente puede rastrearse primariamente a 2018, cuando la Municipalidad de Asunción organizó un foro sobre "ciudades inteligentes y comunidades inteligentes". Allí se presentó como parte del punto 11 del plan "ASU Viva" (Municipalidad de Asunción, 2018), la implementación progresiva de la *smart city*, con sistemas de vigilancia y modernización de la ciudad. Afortunadamente este plan aún no fue concluido. Sin embargo, existen antecedentes locales en torno a la videovigilancia y el reconocimiento facial. El Estado Paraguayo

18 El término y su noción proviene del análisis de Evgeny Morozov (escritor e investigador bielorruso que estudia las implicaciones políticas y sociales de la tecnología): "Dado que reformula todas las situaciones sociales complejas como problemas con definición clara y soluciones definitivas y computables, o como procesos transparentes y obvios a primera vista que pueden optimizarse sin mayor esfuerzo -apenas contando con los algoritmos correctos-, es probable que esta búsqueda tenga consecuencias inesperadas y termine causando más daño que soluciones. A la ideología que legitima y sanciona ese tipo de aspiraciones la llamo "solucionismo". Tomo prestado este término tan peyorativo del mundo de la arquitectura y la planificación urbana, en el que designa una preocupación poco saludable por encontrar soluciones atractivas, monumentales y de mentalidad estrecha (...) a problemas por demás complejos, fluidos y polémicos…" (Morozov, 2015, p. 24)

compró tecnología de vigilancia[19] hace varios años pero se niega a dar información sobre su utilización y mecanismos de tratamiento de los datos. Esa es una clara muestra de la praxis arbitraria del gobierno sobre este tipo de maniobras, razón por la cual existe un real peligro de la posibilidad de aplicar a una escala mayor el tipo de vigilancia que requiere una ciudad inteligente.

Ya hace un par de años, Jean-Marc Offner[20] (2020) escribió que "la idea de que sería posible domesticar un sistema tan complejo como el desarrollo urbano utilizando solo la tecnología ha mostrado sus límites". Estos límites no refieren solamente al tema del urbanismo sino al enfoque de derechos humanos en la planificación. Entonces, ¿cómo encaja la expectativa de privacidad en todo esto?

Para siquiera conceptualizar un proyecto de esta magnitud se debe tener en cuenta que la Corte Interamericana de Derechos Humanos (CorteIDH) refiere en el manual elaborado por Silvia Chocarro (2017) que "los programas de vigilancia son legítimos sólo en casos muy excepcionales. Dado su enorme potencial para invadir y violar la privacidad y la libertad de expresión deben ser cuidadosamente diseñados e implementados, y rigurosamente vigilados. La vigilancia sólo debe aplicarse en circunstancias excepcionales, debe perseguir siempre una finalidad legítima y debe ser la respuesta a un riesgo objetivo, concreto y grave". Esto colisiona de manera frontal con los programas integrales de vigilancia "preventiva" que ya están siendo aplicados por ejemplo en Encarnación («Sistema 911 habilitará 80 nuevas cámaras en Encarnación», 2019) con un sistema con sesenta cámaras de paneo completo (PTZ), diez cámaras de reconocimiento facial y diez cámaras de reconocimiento de placas.

Esta vía ya fue advertida en Estados Unidos, y con especial énfasis en Francia (*La Quadrature du Net*, 2021), dónde la *smart city* se convirtió en un componente de la tecnopolicía (para las prácticas de una fuerza predictiva de crímenes y focos de criminalidad), aunque ello pueda, paralelamente, violentar la privacidad y poner en el foco de la vigilancia a personas inocentes.

Extrapolando esta realidad al Paraguay, es necesario mencionar que al ser aplicados por la policía local estos programas tendrán los mismos vicios que esa institución ya ostenta en la actualidad, aunque se traten de algoritmos y de tecnología "inteligente"; la demarcación de zonas rojas de criminalidad como sinónimo de barrios pobres (Lovera, 2016), entre otras muestras de discriminación, también son un punto clave para abogar por la exclusión de estos sistemas.

Además de esto, Jacques Priol[21] (Leclercq, 2021) indica a la mercantilización de datos de comunidades empobrecidas como el riesgo número uno de la *smart city*, y remarca que todas las personas deben ser protegidas e incluidas en el debate sobre aplicación de cualquiera de estos programas. La tecnología puede ser vital para mejorar las políticas públicas en diversos aspectos, como monitorear y controlar el tratamiento de agua, el tráfico de automóviles o, por supuesto, revisar las redes eléctricas (que ya se aplica mínimamente en Paraguay). No obstante, cuando se trata de vigilancia masiva no se cumplen ninguno de los presupuestos establecidos por las organizaciones internacionales de Derechos Humanos. Estamos hablando de la proporcionalidad: tiene que ver con sopesar los beneficios y los derechos violentados; de la necesidad: en cuanto refiere a que no exista otra vía aplicable ante la situación; y de la legalidad: relacionado a que la actividad del programa se encuentre legislada.

19 En 2019, TEDIC presentó una acción de inconstitucionalidad para obtener información en torno a las compras de equipos de reconocimiento facial y otras tecnologías de vigilancia por parte de organismos estatales. Estos estamentos gubernamentales se negaron sistemáticamente a dar información sobre estas adquisiciones y su utilización. La acción aún no fue resuelta y la disputa sigue vigente.

20 Director general de la agencia de urbanismo de Burdeos Aquitania (a'urba) en Francia.

21 Director ejecutivo y fundador de CIVITEO (Consultora independiente con énfasis en Datos Abiertos y Smart City) en Francia.

Aunque no existen aún estándares internacionales de derechos humanos enfocados específicamente a la *smart city*, Mc Manus et al. (2022) proponen tres pilares como principios rectores para la aplicación de estos programas desde el Estado o las empresas:

PILAR I: El deber del Estado de ofrecer protección contra los abusos de derechos humanos cometidos por terceros, incluidas las empresas, mediante políticas adecuadas, actividades de reglamentación e imposición de sentencias judiciales.

PILAR II: La responsabilidad de las empresas de respetar los derechos humanos, no vulnerando los derechos de terceros, y de remediar las repercusiones negativas sobre los derechos humanos resultantes de sus actividades.

PILAR III: El acceso de las víctimas de abusos de derechos humanos relacionados con las empresas a la reparación mediante mecanismos judiciales o no judiciales.

En el contexto hoy existente no pueden aplicarse con seguridad —entendida como seguridad constitucional— las tecnologías de vigilancia masiva. Cualquier proyecto de ciudad inteligente que pretenda ejecutar estos mecanismos debe tener en cuenta el marco regulatorio de Derechos Humanos. Desde la sociedad civil, en la región en general, existe una preocupación latente que es la misma preocupación que impulsó la redacción de este artículo, y es la capacidad de la *smart city* de violentar los derechos de las personas con la vigilancia. La tecnología es una herramienta eficaz en muchos casos, pero con relación a la vigilancia aún hay muchos puntos para evaluar sobre sus posibles efectos en detrimento de las libertades y su interferencia en la intimidad.

La guía local debe establecer los parámetros de aplicación y prevención de los diversos derechos que se ponen en peligro: derechos a la intimidad y a la libertad de pensamiento, expresión y asociación. Como se puede comprobar a lo largo de los diversos informes internacionales, la adquisición y uso de tecnologías que permiten la vigilancia a escala masiva por parte de los Estados está en auge en la región. Sin embargo, como la ley no avanza a la misma velocidad que esta tecnología, estos programas podrían someter a las personas a una vigilancia indiscriminada. Sin ninguna herramienta para la protección efectiva de los derechos y con el Estado justificando estas prácticas con la *smart city* y el desarrollo urbano, vale la pregunta: ¿Quién vigila a los vigilantes?[22]

22 "Who watches the watchmen?", del cómic "Watchmen" de Alan Moore y Dave Gibbons.

Referencias

1. Chocarro, S. (2017). *Estándares internacionales de libertad de expresión: Guía básica para operadores de justicia en América Latina.* CIMA. https://www.corteidh.or.cr/tablas/r37048.pdf

2. La Quadrature du Net. (2021, junio 11). Le mythe participatif de la Smart city et de sa surveillance. *La Quadrature du Net.* https://www.laquadrature.net/2021/06/11/le-mythe-participatif-de-la-smart-city-et-de-sa-surveillance/

3. Leclercq, B. (2021). Web in the city. *Libération*. https://www.liberation.fr/forums/web-in-the-city-20210415_PLREEG2JFNGPJI26QSZPPAXFKM/

4. Lovera, D. O. (2016). La criminalidad y sus determinantes en el Paraguay. *Población y Desarrollo, 16*(30), Art. 30.

5. Mc Manus, A., Noguera, A., & Smart, S. (2022). *Smart Cities y derechos humanos* (pp. 319-368).

6. Morozov, E. (2015). *La locura del solucionismo tecnológico* (Primera edición). Katz.

7. Municipalidad de Asunción. (2018, abril 11). *DEBATEN SOBRE CIUDADES INTELIGENTES, MODERNIZACIÓN Y DESCENTRALIZACIÓN MUNICIPAL Y PARTICIPACIÓN CIUDADANA.* Municipalidad de Asunción. https://www.asuncion.gov.py/asu-viva-municipalidad/debaten-ciudades-inteligentes-modernizacion-descentralizacion-municipal-participacion-ciudadana

8. Offner, J.-M. (2018). La smart city pour voir et concevoir autrement la ville contemporaine. *Quaderni: la revue de la communication, 96*, 17-27.

9. Offner, J.-M. (2020). IV. Accès aux ressources et civilité. En *Anachronismes urbains* (pp. 79-99). Presses de Sciences Po.

10. Sistema 911 habilitará 80 nuevas cámaras en Encarnación. (2019, agosto 20). *Agencia IP.* https://www.ip.gov.py/ip/sistema-911-habilitara-80-nuevas-camaras-en-encarnacion/

ANÁLISIS DE UN AMPARO EN POS DE LA PROTECCIÓN DE DATOS PERSONALES

Álvaro Penayo Ovelar & Alfredo Daniel Barrios Duarte

ANÁLISIS DE UN AMPARO EN POS DE LA PROTECCIÓN DE DATOS PERSONALES

— por Álvaro Penayo Ovelar[23] & Alfredo Daniel Barrios Duarte[24]

En julio del 2018 el Ministerio del Interior y la Policía Nacional iniciaron un proceso de innovación en el Sistema 911 en Asunción y en el Área Metropolitana. El plan implica, según medios de comunicación, implementar cámaras de vigilancia con tecnología biométrica (reconocimiento facial). A raíz de ello, en 2019 la abogada Maricarmen Sequera Buzarquis, en su rol de agente del TEDIC, requirió al Ministerio del Interior, a través del Portal Unificado de Acceso a la Información Pública, datos sobre diversos puntos del proyecto. El 26 de abril del 2019 el Ministerio del Interior contestó a la solicitud de la Abg.[da] Sequera, respondiendo parcialmente a algunos de sus planteamientos y, fundado en una resolución emitida previamente por el mismo órgano, negándose a responder a los demás por supuesta razón de confidencialidad. En consecuencia, la abogada promovió un amparo en los términos de la Acordada 1005/2015 de la Corte Suprema de Justicia para obtener tutela de los derechos otorgados a la ciudadanía por la Ley 5282/2014.

La acción promovida por la Abg.[da] Sequera Buzarquis recayó en el IX Juzgado Penal de Garantías de la Capital, configurándose así la primera instancia con el expediente caratulado como *"Amparo constitucional promovido por la señora Maricarmen Sequera Buzarquis bajo patrocinio de los abogados Federico Legal Aguilar y Ezequiel F. Santagada c/ el Ministerio del Interior* (nro. 609, año 2019)". Por sentencia del 1 de agosto del 2019, el Juzgado desestimó la pretensión de la amparista, quien apeló la decisión. El 28 de agosto del 2019, el *ad quem*, Trib. de Apel. Penal de la IV Sala de la Capital, confirmó la sentencia de primera instancia. Y si bien la amparista recurrió a la casación, a la fecha de la redacción de este ensayo no hay aún sentencia de la máxima instancia judicial.

En ese contexto, este ensayo presenta argumentos a favor de la pretensión de la amparista en el caso mencionado, discrepando así con las consideraciones de los juzgadores de primera y segunda instancia. Consideramos que el amparo es procedente y el derecho merece ser atendido por tres motivos: los intereses difusos en juego, la inexistencia de otras vías sino el amparo y la imposibilidad (contemporánea a los hechos descritos) de subsanar la cuestión por vías administrativas. A continuación, desarrollaremos cada uno de estos puntos.

1. El caso es de interés difuso, ajustándose al ejercicio de una acción de amparo

El artículo 134 de la Constitución Nacional establece la acción de amparo. De acuerdo con él, el amparo será «… de acción popular para los casos previstos por la ley». Esto significa que la protección de los derechos difusos, también reconocidos en la Constitución (art. 38), puede ser reclamada por la vía del amparo. Sin embargo, ¿se trata la pretensión del caso analizado de un derecho difuso? Creemos que sí.

Comentando el artículo 38 de la Constitución, la jurista nacional Garay de Vouga (1997) se propone definir qué se entiende por intereses difusos. La autora cita las siguientes definiciones: «El interés difuso es aquel que pertenece indistintamente a una pluralidad de sujetos ligados por la pretensión de goce de una misma prerrogativa relativa a bienes indivisibles que por esta misma razón no son susceptibles de apropiación individual» (def. de Morello); «[Los intereses difusos] pertenecen a una serie

23 Estudiante de la carrera de Derecho en la Universidad Nacional de Asunción (UNA). Dactilógrafo en un Juzgado en lo Civil y Comercial - Capital. alvaropenayoo@gmail.com

24 Estudiante de la carrera de Derecho en la Universidad Nacional de Asunción (UNA). Asistente legal. barriosalfredo336@gmail.com

indeterminada de individuos de difícil e imposible determinación y su referencia a un bien indivisible con el que se hallarían en una especie de comunión tipificada por el hecho de que la satisfacción de todos, así como la lesión de uno solo, constituye, *ipso facto*, lesión a la entera colectividad» (def. de Barboza); «El interés difuso no pertenece a persona determinada ni a grupos determinados de personas, sino a toda la sociedad» (def. de Marienhoff).

La implementación de cámaras de vigilancia con tecnología de reconocimiento facial en espacios públicos afecta directamente al derecho a la privacidad. Este derecho es de índole social, pues la satisfacción de este derecho, así como su violación, al darse continua e indiscriminadamente en espacios públicos y comunes, o lesiona o satisface a todos sus usuarios. Es esta la razón por la que se recomienda la realización de estudios de campo en cada comunidad en particular antes de proceder a la implementación de dicha tecnología (Fontes & Perrone, s. f.). En efecto, uno de los requerimientos iniciales formulados por la amparista, ante el riesgo presente y real de lesión a la privacidad de todos los usuarios de la vía pública, fue el de obtener declaración sobre si estos estudios fueron hechos o no antes de la implementación de las cámaras de vigilancia biométrica.

Además, el acceso a la información pública es un derecho de interés difuso cuyo ejercicio aquí ha sido violentado. El simple carácter de fuente de información pública, que justifica la sujeción del demandado a la Ley 5282/14, bastaría para acreditar el interés social y público en la información. No se trata de un agravio particular e individual de la amparista (lo cual es reconocido por la sentencia de segunda instancia), sino de la lesión en un caso determinado de un derecho fundamental (carácter reconocido por la Corte Suprema de Justicia a este derecho en su Acordada 1005) y colectivo (recuérdese la citada definición de Barboza).

Que el requerimiento haya sido efectuado —y la denegación sufrida— por una persona en particular, quien en consecuencia invoca el amparo del derecho, no menoscaba el interés público y difuso en la pretensión de la amparista. Sin embargo, el juzgador de segunda instancia se enfoca en precisar la existencia de agravios sufridos o no por la amparista, y deja de atender los sufridos por la comunidad. La lesión de derechos colectivos no se puede dar sino con la reiteración sucesiva de casos particulares, y el presente se puede, sin duda, considerar como uno de ellos. No podría la comunidad ejercer la acción para defenderse de estas lesiones en un litisconsorcio desorganizado e inconcebible, por lo cual ello se debe hacer a través de particulares u organizaciones que actúen en representación del cuerpo social. No se aplica el mismo razonamiento usado en la sentencia en casos de lesiones a otros derechos universalmente reconocidos como difusos, como el derecho a la seguridad social.

Para finalizar este punto, nuevamente citemos a la autora paraguaya Garay de Vouga (1997), quien tiene dicho que «dado entonces que el artículo 38 de la Constitución incorporó entre los derechos del ciudadano el de la defensa de los intereses difusos, queda expedita la posibilidad de demandar su protección por medio del amparo», respaldando así la afirmación que la protección de los derechos difusos debe revestir la figura del amparo.

2. No existe otra figura jurídica por la cual se pueda llevar adelante la acción

La Acordada 1005 de la Corte Suprema de Justicia resolvió que «… para el caso de denegación expresa o tácita de una solicitud de acceso a la información, la acción judicial tramite según las reglas previstas en el artículo 134 de la Constitución y en el Código Procesal Civil para el juicio de amparo». Esto quiere decir que la misma Corte establece que los procesos contenciosos a raíz de la aplicación de la ley de acceso a la información pública incoados ante sus órganos se realicen a través de acciones de amparo.

El pedido de la amparista fue formulado a través del Portal Unificado de Información Pública, creado por Decreto 4064/2015 del Poder Ejecutivo, que reglamenta la Ley 5282/2014 De libre acceso ciudadano a la información pública y transparencia gubernamental. La ley reglamentada con el citado decreto es la referida en la Acordada 1005. Consecuentemente, las solicitudes de acceso a la información pública formuladas en el portal creado para la aplicación de esta ley son también las que, por su denegación expresa o tácita, viabilizan la acción de amparo en los términos de la acordada. Además, por la naturaleza de los requerimientos y el órgano interpelado, el pedido formulado por la amparista debería considerarse una solicitud de acceso a información pública.

Por lo tanto, no se pudo haber interpuesto la acción bajo otro instituto más que el amparo. Denegada tácitamente la solicitud de la amparista (pues así debe entenderse respecto de los puntos no respondidos), la máxima instancia del Poder Judicial dispone que el procedimiento se debe tramitar según las reglas del amparo.

La existencia y las disposiciones de la Acordada 1005 son expresamente reconocidas por los juzgadores de segunda instancia. Sin embargo, invocando el art. 136 de la Constitución, juzgan el mérito de la pretensión de la amparista según los requisitos que ordinariamente debería reunir una acción de amparo para ser atendida. Esto va en contraposición a la acordada de la Corte, la cual establece que los procedimientos nacidos en virtud de solicitudes de acceso a información pública denegadas sean tramitados por la vía procesal del amparo, y no que sean juzgadas como tales.

3. Porque sí se agotaron las vías administrativas

Incluso si la pretensión de la amparista fuere juzgada según las reglas que ordinariamente requiere un amparo para ser procedente, la acción tiene los méritos suficientes para ser atendida. Uno de estos requisitos, según jurisprudencia de los tribunales de la República, es el agotamiento de las vías administrativas. Ello se establece en el siguiente apartado: «… se tiene que dichos requisitos [para la procedencia del amparo], establecidos en la propia norma constitucional, son: … d) que se hayan agotado las vías administrativas previas, en los casos que se recurra en amparo contra decisiones de entidades, sean públicas o privadas…» (Acuerdo y Sentencia 5, del 18 de febrero de 2021. Tribunal de Apelación en lo Civil y Comercial, Segunda Sala de la Capital, op. de Juan Carlos Paredes Bordón). La amparista sí agotó las vías administrativas antes de interponer la acción, no quedando otra vía para reclamar el derecho (ver punto 2) sino el amparo.

Debe considerarse que la vía administrativa agotada es la formulación de la solicitud a través del Portal Unificado de Acceso a la Información Pública creado por Decreto 4064/2015. En consecuencia, no podrá alegarse que debe hacerse el requerimiento a través de mecanismos internos de la entidad requerida (en el caso, el Ministerio del Interior). Esto sería complicar innecesariamente el procedimiento; y es precisamente lo que el Portal, por ser unificado, intenta evitar. Además, el decreto men-

cionado sujeta al Ministerio del Interior a utilizar el Portal en él creado (art. 8), pues el Ministerio no tiene autonomía funcional, ya que las entidades con autonomía funcional deben crear sus propias plataformas por disposición del mismo artículo.

Siendo el Portal Unificado de Acceso a la Información Pública la vía administrativa del Ministerio del Interior establecida por el decreto reglamentario de la Ley 5282/2014, la solicitud formulada en él y su posterior denegación deben entenderse como el agotamiento previo de las vías administrativas. Esto da venia a la hoy amparista para interponer la acción de amparo en los términos de la Acordada 1005 de la Corte Suprema de Justicia.

Tampoco podría alegarse que no se agotaron las vías administrativas por no haberse interpuesto los recursos administrativos previstos en la Ley 6715/2021, De Procedimientos Administrativos. Esta ley prescribe que deberán agotarse los recursos administrativos de reconsideración y de jerarquía antes de quedar expedita la vía judicial en lo contencioso-administrativa, al recurrir un acto individual de la administración pública. No obstante, la ley fue dictada con posterioridad a la interposición del amparo. Así también, aunque la ley mencionada no crea dichos recursos, es la que por primera vez dispone que la vía administrativa se entenderá agotada solamente una vez interpuestos los recursos de reconsideración y jerarquía.

Además, al haber emanado del máximo jerarca del Ministerio del Interior la resolución que dispone responder parcialmente a los cuestionamientos de la amparista, no cabría racionalmente interponer un recurso jerárquico contra la resolución en los términos del art. 66 de la Ley 6715/2021. De ello se desprende que, aplicando los art. 65 *in fine* y 68 de la misma ley, la vía judicial queda expedita, aunque el caso que nos ocupa no versa sobre asuntos de lo contencioso-administrativo.

Por lo tanto, resolver que el amparo es improcedente por no haberse agotado las vías administrativas previas, no habiéndose interpuesto un recurso de reconsideración contra la resolución que niega los requerimientos de la actora, sería manifiestamente arbitrario. Los hechos que nos ocupan se dieron entre el 2018 y el 2019, mientras que la Ley 6715/2021 (que prescribe el agotamiento de las vías administrativas, estableciendo que por tales se entienden los recursos de reconsideración y jerarquía, previa acción judicial) fue promulgada dos años después de la resolución por la que se agravia la actora, y entró en vigencia en 2022.

De hecho, ni siquiera los juzgadores de primera y segunda instancia entendieron que estos recursos debían interponerse; incluso la propia resolución de primera instancia menciona, en su análisis sobre la procedencia ordinaria de un amparo, que las vías administrativas deben agotarse si ellas cupieren. Esto demuestra que el juzgador estaba consciente de este requisito ordinario y que no consideró que el amparo era improcedente por faltar aquél, pues el rechazo se basó en otras consideraciones, al igual que en segunda instancia.

Conclusión

La tutela judicial del derecho de acceso a la información pública en los términos de la Ley 5282/2014 debe necesariamente darse en el marco de una acción de amparo, pues así lo establece la Acordada 1005 de la Corte Suprema de Justicia. Invocar otra figura procesal con este fin se traduciría muy probablemente en el rechazo *in limine* de la acción, ya que los jueces no podrían ignorar la existencia de la reglamentación hecha por la Corte Suprema ni tampoco podrían juzgar la constitucionalidad de ella. De esta manera, la misma Corte Suprema de Justicia determina que, aunque no se tratare de lo que ordinariamente se consideraría como una acción de amparo, los reclamos fundados en la Ley 5282/2014 deberán ser tramitados según el proceso de dicha garantía constitucional.

El resultado es una situación muy complicada en la que los usuarios de justicia y los mismos magistrados deberán encontrar la manera de atender los reclamos relacionados al acceso a la información pública en el marco de una acción de amparo. Pronto se hace presente la cuestión de si, no siendo propiamente acciones de amparo, deberían estos procesos ser juzgados utilizando los mismos criterios aplicados al analizar la procedencia o no de un amparo cualquiera; criterios muchas veces no reunidos en su totalidad en los casos de reclamos fundados en la Ley 5282/2014.

El caso que aquí nos ocupa, por tratarse de un litigio en relación al acceso a la información pública, cae bajo la previsión de la Acordada 1005. En consecuencia, el proceso debe transitar la vía del amparo, por más de que, en ausencia de la Acordada, pudiera no ser —de ordinario— procedente bajo dicha figura. Entonces, sería una injusticia que los jueces se limiten a rechazar la acción por no reunir los criterios que un amparo debería natural y comúnmente reunir, pues ello significaría que la Corte Suprema de Justicia condenó al rechazo a la gran mayoría (¡si no a todos!) de los reclamos hechos en el ámbito de la Ley 5282/2014. Es evidente que este no fue el propósito de la Acordada, sino, muy al contrario, garantizar la tutela efectiva del derecho al acceso a la información pública al designar el proceso sumario y gratuito del amparo como vía procesal para estos reclamos.

Aun así, esperamos con este ensayo haber demostrado que, incluso si se juzgase la procedencia de la acción que analizamos aquí particularmente según los criterios naturales y ordinarios del amparo, ella sería procedente. Esto porque la defensa de derechos difusos, como aquí sucede, solamente reconoce como vía al amparo en nuestro medio, y todo otro instituto procesal implicaría su rechazo por falta de legitimación activa. Además, no hay otra figura procesal por la que intentar la defensa del derecho, ni el habeas data ni *habeas corpus* son aptos, y ni siquiera la vía contencioso-administrativa lo es, pues la Acordada 1005 de la C. S. J. estableció como vía al amparo. Así también, debe entenderse que en este caso se agotaron las vías administrativas previas (requisito ordinario para la procedencia de un amparo), con la importante salvedad de que al momento de los hechos en los que se funda el litigio no había entrado en vigor aún la Ley 6715/2021.

Referencias

1. Fontes, C., & Perrone, C. (s. f.). *Ethics of surveillance: Harnessing the use of live facial recognition technologies in public spaces for law enforcement.* 11.

2. Garay de Vouga, M. (1997). *La defensa de los intereses difusos.* En Camacho, E.; Lezcano, L. Comentario a la Constitución - Tomo I: Homenaje al Quinto Aniversario. Corte Suprema de Justicia (https://www.pj.gov.py/ebook/libros_files/Comentario_a_la%20Constitucion_%20Tomo_I.pdf).

3. Acuerdo y Sentencia 5, del 18 de febrero de 2021. Tribunal de Apelación en lo Civil y Comercial, Segunda Sala de la Capital, op. de Juan Carlos Paredes Bordón.

Tecnología
& Derechos
Humanos