Anuario de Derecho N° 48-2019 – Año XXXIX - ISSN 0553-0814
Edición anual diciembre 2018-noviembre 2019
Págs. 254-265

N. AUTORES INTERNACIONALES INVITADOS

Protección de Datos Personales y Derecho: Tendencias Modernas en el Derecho Comparado -Comentarios al Proyecto de Ley No. 463 de 2017-

RUBÉN E. RODRÍGUEZ SAMUDIO*
Universidad de Hokkaido, Japón
E-mail: ruben18@juris.hokudai.ac.jp

RESUMEN

Panamá se encuentra rezagada en materia de protección de datos personales. El reciente intento de aprobar una ley sobre esta materia culminó con un rechazo del proyecto de ley y su envío al órgano ejecutivo para implementar los cambios recomendados durante el proceso legislativo. Este artículo compara el proyecto de ley con diversas legislaciones extranjeras que regulan la protección de datos personales. Si bien el proyecto se convierte en un punto de partida, es necesario reconocer que el mismo carecía de muchos principios comunes que pueden encontrarse en el derecho comparado. Tales falencias que impiden el objetivo que se pretendía alcanzar mediante su aprobación. Por ende, resulta necesario reafirmar las metas y obligaciones de Panamá en la materia y establecer normas que se adecúen los estándares reconocidos a nivel mundial.

PALABRAS CLAVE

Protección de Datos, Privacidad, Internet, Derecho Comparado

SUMMARY

Panama has fallen behind in the subject of personal data protection. The recent attempt to pass a law on the subject ended with the rejection of the bill and its return to the executive branch to add the recommendations made during the legislative process. This paper compares the bill with various foreign laws that regulate personal data protection. While the bill serves as starting point nevertheless it must be said that it lacked various common principles found in comparative law. Such failings would become an obstacle to achieve the goals established therein. Thus, it is necessary to reaffirm the goals and obligations of Panama regarding this matter and to establish rules that are in line with recognized global standards.

KEYWORDS

Data Protection, Privacy, Internet, Comparative Law.

---

* *Doctor en Derecho, Universidad de Hokkaido, Japón.*
Profesor asistente de la Universidad de Hokkaido, Japón.
Abogado de la República de Panamá.
Correo electrónico: rubenr1618@gmail.com, ruben18@juris.hokudai.ac.jp

INTRODUCCIÓN

Este artículo tiene por objeto analizar el proyecto de ley sobre la protección de datos de carácter personal en base a la situación actual de la protección a la información personal desde la perspectiva del derecho comparado y los retos jurídicos a los que se enfrenta Panamá en esta materia. En la actualidad Panamá se encuentra rezagado en cuanto a otras legislaciones en lo referente a la protección de datos de carácter personal. El Proyecto de Ley No. 463 de 2017 fue devuelto al órgano ejecutivo y se encuentra a la espera de modificaciones para atender las recomendaciones surgidas del proceso legislativo. Con tan sólo 37 artículos es una de las leyes más cortas que buscan regular una materia tan importante como la protección de los datos personales. A pesar de que el proyecto no fue adoptado por el órgano legislativo consideramos prudente realizar algunos comentarios sobre el mismo esperando así que cualquier futuro esfuerzo en legislar la materia resulte exitoso. Si bien es cierto el proyecto no es extenso hemos decidido enfocar este trabajo únicamente en algunos principios generales sin entrar a discutir aspectos referentes a las instituciones encargadas de velar por el cumplimiento de la ley o su organización.

El control que tiene un individuo sobre sus datos personales se ha vuelto un tema de fundamental importancia a raíz de la creación de medios informáticos electrónicos que tuvo lugar durante la segunda mitad del siglo XX ha resultado en un cambio social que se ve reflejado tanto a nivel individual como grupal. Esta dinámica individuo-información y su efecto en políticas estatales tiene sus orígenes en la década de los 60 como respuesta de los estados industrializados al desarrollo e implementación de las computadoras, sin embargo, no fue hasta la década de los 70 cuando este tema adquiere independencia como tema de políticas estatales independientes y surgen leyes especiales sobre la materia.[1] Existen también dificultades al momento de nombrar la rama jurídica que estudia la protección de datos. Bennett comenta que en las legislaciones de países angloparlantes se aborda el tema bajo el término *privacy* o privacidad, en consideración de las connotaciones técnicas del término protección de datos.[2] Sin embargo, la tendencia en Latinoamérica, Europa y algunos países asiáticos es utilizar el término protección de datos personales o términos similares.

El termino era digital o era de la información recoge tales cambios y les otorga una característica trascendental propia de otros grandes cambios históricos. Sin embargo, y a diferencia de la revolución industrial, la revolución digital presupone una superación tecnológica desconocida hasta el momento. Atrás quedan declaraciones como la emitida por Henry Ellsworth, director del departamento de patentes de Estados Unidos, quien en un reporte al congreso norteamericano en 1843 manifiesta que "el avance de las artes cada año riñe con nuestra credulidad y parece presagiar la llegada de un periodo en el cual la autosuperación humana ha de terminar". Si bien las palabras de Ellsworth son consideradas como una licencia literaria que busca enfatizar la elevada carga de trabajo que afrontaba la oficina de patentes de Estados Unidos la idea de un límite al desarrollo tecnológico parece impensable en el mundo moderno. No obstante, las sociedades de información, no son la causa de los problemas relativos a la recolección de datos, sino únicamente el contexto dentro del cual estos se presentan, particularmente en relación con instituciones gubernamentales

[1] Bennett (1992) pag. 2
[2] Bennett (1992) pag. 13

y como estas administran y procesan datos personales de los ciudadanos.[3] Uno de los desafíos más importantes es el control que los individuos tienen sobre su información personal, particularmente cuando se tiene en cuenta que actualmente es posible almacenar una gran cantidad de información personal en medios físicos, como memorias USB, o en servidores en la Internet, conocidos como la nube o *cloud.*

En 2014, en un reporte titulado *Data Protection Principles for the 21st Century*, el Oxford Internet Institute describe que desde un punto de vista práctico, la tendencia moderna en la recolección de datos debe transferir la responsabilidad de los individuos hacia los sujetos que recogen los datos y aquellos que la utilizan y cuya responsabilidad debe establecerse en base a como administran y procesan la información en lugar a la manera en que obtienen el consentimiento del individuo para la recolección de la misma.[4] No obstante, estas recomendaciones fueron propuestas antes de que se descubriera la recolección de forma anónima y sin el consentimiento de los titulares por parte de la compañía de consultoría política Inglesa *Cambridge Analytica* que tuvo acceso información personal contenida en *smartphones* por medio de redes sociales, Facebook en particular, constituyéndose así en la noticia más grande del 2018 en el tema de protección de datos. Utilizando la información recolectada esta compañía fue capaz de ejercer influencias en elecciones de varios niveles a lo largo del mundo, incluyendo países como Inglaterra, India y Estados Unidos por mencionar solo algunos.[5]

Por otra parte, tampoco es extraño encontrar ejemplos en los que el uso que la compañía da a la información recolectada no es del todo claro. Los usuarios han ido poco a poco convirtiéndose en el producto. La aparición de *smartphones* y el posterior desarrollo de aplicaciones que hacen uso de la información personal que tales dispositivos colectan como parte de sus funciones. En muchos casos, los usuarios finales acceden a la recolección de tales datos al momento cuando instalan las aplicaciones o bien mediante su uso. No es raro leer noticias sobre compañías que manejan grandes volúmenes de información personal que resultan blanco de ataques informáticos cuyo fin es obtener datos como direcciones o números de tarjeta de crédito las cuales son utilizadas en transacciones fraudulentas. No obstante, la dinámica jurídico-informática no puede limitarse únicamente al uso de la información por entes corporativos. Google y Wikipedia han cambiado la manera en que el ser humano accede a la información, y algunos estudios apuntan han tenido efecto en la manera en la que el cerebro humano conserva y hace uso de esta.[6] Es por eso las discusiones doctrinales de la relación derecho-información en la era digital no pueden limitarse a temas tradicionales como derecho de propiedad intelectual o protección de secretos industriales, sino que debe expandirse para incluir el rol del individuo y su derecho al manejo de su información personal desde la perspectiva de los derechos a la imagen, a la privacidad y en los últimos años el

---

[3] Bennett (1992) pag. 17-18

[4] *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* (2014) 8

[5] El escándalo de Cambridge Analytica tuvo sus inicios con dos artículos publicados en el New York Times y el Observer. Según las investigaciones de estos diarios la compañía consultora utilizo una aplicación para recabar información no solo de las personas que la instalaron en sus teléfonos, sino además de sus contactos, llegando a recolectar información de alrededor de 50 millones de personas. Tal información fue utilizada para influir en elecciones presidenciales como la de Estados Unidos en 2016 y referéndums como el voto de Brexit.
New York Times (2018), The Observer (2018)

[6] Huffington Post (2015)
Scientific American (2013)

derecho a ser olvidado. Panamá no escapa a estas realidades, debiendo hacer frente a los cambios de las relaciones sociales y del individuo con su propia información. Es por esto por lo que este artículo utiliza leyes de diferentes jurisdicciones con el fin de analizar las normas del proyecto de ley desde la perspectiva del derecho comparado.

PRINCIPIOS GENERALES

La principal función de una ley general de protección de datos es servir como guía a instituciones públicas y privadas al momento de recolectar, trasmitir, divulgar, procesar o manejar de cualquier manera información de carácter personal. Es por esto por lo que, si bien muchas leyes establecen derechos y obligaciones específicos estos son desarrollados dentro de un núcleo central que se constituye como norte en el tratamiento de datos personales. La *Data Act* sueca de 1973 es considerada como la primera ley que específicamente aborda la materia de protección de datos.[7] Para el año 2011, existían 76 países con leyes de protección de datos y a 2017 la cifra aumento hasta alcanzar los 120.[8] A nivel supranacional encontramos por ejemplo los *Guidelines on the Protection Of Privacy and Transborders Flows of Personal Data* adoptados por la OECD en 1980 y actualizados por última vez en 2013. En su versión actual de 2013, estas reglas generales están compuestas por ocho principios: principio de recolección limitada, de calidad de los datos, de especificación del propósito, de limitación de uso, de seguridad de los datos, de transparencia, de participación de los individuos y finalmente el principio de rendición de cuentas.[9] Si bien los principios son los mismos consagrado en la versión original de 1980, su interpretación y ámbito de aplicación ha ido cambiando de la mano del desarrollo tecnológico.

Un examen de las varias legislaciones revela que la tendencia en el derecho comparado es tener una ley general que establezca los principios generales en cuanto a la información personal.[10] [11] En Uruguay, Colombia y Argentina consagran en sus leyes principios generales como lo son el principio de licitud, libertad, legalidad, transparencia, veracidad, finalidad, seguridad y otros similares. Estas leyes no se limitan a enumerar estos principios, sino que los desarrollan de manera que sean de fácil entendimiento y aplicación aun cuando no haya una norma específica aplicable al caso. Estados Unidos por su parte no tiene una sola ley a nivel federal que regule de manera general la recolección de datos personales, prefiriendo una regulación por materias con apoyo de las normas individuales de cada estado. No obstante, a nivel federal encontramos los *fair information practice principles* de la Comisión Federal de Comercio de Estados Unidos. Estos principios fueron propuestos por primera vez en 1973 en un reporte del Departamento de Salud

---

[7] Greenleaf (2011) pág. 1.
[8] Greenleaf (2017) pág. 10.
[9] OECD (2013) págs. 14-15, *THE OECD PRIVACY FRAMEWORK*
http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
[10] Bennett (1992) pág. 3
[11] Las referencias que en este trabajo se hagan a legislaciones extranjeras hacen referencia a las siguientes leyes:

Argentina	Ley No. 25236 de 2000
Canadá	Personal Information Protection and Electronic Documents Act
Estados Unidos	Privacy Act de 1974 (5 U.S.C. § 552a)
Colombia	Ley Estatuaria 1581 de 2012
Japón	Ley No. 57 de 2003
Reino Unido	Data Processing Act de 2018
Reglamento (Ue) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016	
Uruguay	Ley 18331 de 2008

titulado *Record Computers and the Rights of the Citizens*[12] como respuesta al desarrollo de tecnologías de recolección de información. Los principios se presentan en pares, a saber: de notificación y conocimiento, elección y consentimiento, acceso y participación, integridad y seguridad, y por último aplicación y reparación.

A nivel europeo a partir de mayo de 2018 entró en vigor Reglamento General de Protección de Datos (en adelante RGPD) que busca establecer reglas generales dentro del sistema de la unión europea. El segundo capítulo del RGPD trata sobre los principios relativos a la protección de datos y dispone que los datos personales serán tratados de manera lícita, leal y transparente, siendo recogidos para fines determinados explícitos y legítimos en una medida adecuada, pertinente y limitada en base a esos fines además de ser exactos y actualizados de ser necesario. También establece un principio de temporalidad ya que requieren que los datos sean mantenidos durante no más tiempo del necesario, aunque reconoce que podrán conservarse por mayor tiempo por fines de interés público.

Finalmente establece un principio de seguridad no solo contra la perdida, destrucción o divulgación de los datos, sino contra accesos no autorizados y establece la responsabilidad en cuanto al cumplimiento de estos principios en el responsable de tratamiento de los datos. Los RGPD no solo enumeran estos principios, sino que también los desarrollan, estableciendo las pautas concretas para que los mismos se consideren como cumplidos. Debemos mencionar también que el artículo 45 de los RGPD solo permite la transmisión de datos a un tercer país u organización internacional cuando la Comisión determine que el país u organización en cuestión garantizan un nivel de protección adecuado y dicha determinación se hará tomando en cuenta elementos como el estado de derecho, el respeto a los derechos humanos y garantías fundamentales entre otros. La ley japonesa consagra una serie de políticas concernientes a la protección de datos personales que cubren instrucciones básicas en cuanto a la promoción de protección de datos personales, asuntos generales relativos a la protección de datos personales por parte del Estado, gobiernos locales, entidades administrativas constituidas en sociedades o no, así como asuntos generales relativos a la protección de datos personales por parte de compañías privadas, la pronta resolución de quejas relativas a la protección de datos personales y finalmente cualquier otro punto que tenga que ver con la protección de tales datos.

El proyecto de ley inicia proclamando que su objetivo es establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales en consideración a su relación con la vida privada y demás derechos fundamentales de los ciudadanos. Ya en este punto surgen interrogantes con respecto al ámbito del ámbito de aplicación de este ya que se hace referencia únicamente a ciudadanos, sin embargo, la constitución nacional le reconoce estos derechos fundamentales tanto a nacionales como extranjeros. Pero la mayor deficiencia del proyecto es no determinar cuáles son estos principios rectores que pretende establecer, si bien algunas obligaciones y principios pueden inferirse de la redacción de artículos posteriores, el proyecto no presenta una lista de estos por lo que tampoco los desarrolla. También llama la atención que el segundo artículo del proyecto entra a establecer las excepciones a la aplicación de las normas contenidas en el mismo. Si bien se trata de una mera cuestión de orden, consideramos que se presa a confusiones en cuanto a las prioridades de la norma.

[12] Un archivo del reporte puede encontrarse en: https://www.justice.gov/opcl/docs/rec-com-rights.pdf Fecha de acceso: 26 de agosto de 2018.

DATOS DE CARÁCTER PERSONAL

Las leyes de protección de datos tienden a definir datos personales de una manera amplia. Por ejemplo, el Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 establece que dato de carácter personal estableciendo se refiere a cualquier información relativa a una persona física identificada o identificable. Está definición es recogida por las leyes de Argentina, Uruguay y Colombia adoptan una definición similar a la establecida por el Convenio No. 108 del Consejo de Europa. La RGPD define datos personales como toda información sobre una persona física identificada o identificable , definiendo persona física identificable como toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. El Reino Unido adopto el RGDP en su legislación interna y define información personal toda información relativa a un individuo vivo, identificado o identificable.

Japón define dato de carácter personal como toda información sobre una persona viva que sirva para identificar a tal individuo por su nombre fecha de nacimiento o cualquier otra descripción contenida en dicha información. Cabe señalar que la ley otorga protección no solo a los datos personales, sino a cualquier información relacionada que pueda servir para identificar los datos personales, otorgando un doble nivel de protección. En datos personales es toda información relacionada con un individuo vivo, pero la ley también incluye una definición para datos personales relacionados con la salud (*personal health information*) la cual se extiende a individuos fallecidos y comprende información relacionada a la salud física y mental, así como cualquier otra información que se obtenga directamente o indirectamente de tratamientos médicos a los que se someta el individuo.

El proyecto de ley se decanta por una definición amplia de dato de carácter personal al establecer que es cualquier información concerniente a personas naturales, que las identifica o las hace identificables. Siguiendo la tendencia encontrada en las legislaciones consultadas, el proyecto adopta definiciones para varios tipos de datos, no obstante, nos referiremos únicamente al dato anónimo y dato disociado ya que consideramos que las definiciones presentadas se prestan para confusión ya que estos dos términos no aparecen en ningún otro artículo de la ley, por lo que su ámbito de aplicación y su objetivo no resulta claro. El dato disociado es aquel que no puede asociarse con su titular, ni permite que la persona natural sea identificada por razones de la estructura, contenido o grado de desegregación. Por su parte, el dato anónimo es aquel dato cuya identidad no puede ser establecida por medios razonables, o el nexo entre el mismo y la persona a la que se refiere. En cuanto al dato disociado, parece referirse a datos estadísticos, como aquellos recolectados en investigaciones científicas. De ser este el caso, el dato pierde su característica de personal, por lo no entraría en el ámbito de aplicación de la ley. Sin embargo, la definición de dato anónimo también parece hacer referencia a este tipo de datos y su estructura lógica se presta para confusiones. En primer lugar, no es claro a que se refiere la ley cuando habla de identidad del dato en relación con los datos anónimos. A nuestro parecer existen dos posibles acepciones de la palabra identidad en este caso. En primer lugar, podría entenderse como la información personal del individuo en cuestión (nombre, fecha de nacimiento etc.) En segundo lugar, identidad podría

referirse a otras características del dato en general (su formato, su fuente, tamaño, etc.). Sin embargo, en este último caso surge la duda de cómo puede considerarse como dato tal si tal información es desconocida. Por otra parte, si el dato anónimo hace referencia a la información personal del individuo debe considerarse que los datos anónimos y los dato disociados son términos sinónimos. Otra confusión nace de la segunda parte de la definición de dato anónimo la cual se refiere al nexo entre el dato y la persona a la que se refiere. Si tal nexo es desconocido, no se comprende cómo puede considerarse el dato como de carácter personal, bajo las definiciones que la misma ley, si desconoce la información personal del individuo y el nexo entre el dato y la persona en cuestión estaríamos frente a datos estadísticos. Finalmente, el proyecto de ley guarda silencio sobre datos de salud, biométricos, genéticos, y otros relativos a la identidad física y genética del individuo por lo que no podemos comentar al respecto.

CONSENTIMIENTO E INFORMACIÓN EN LA RECOLECCIÓN Y TRANSMISIÓN DE DATOS PERSONALES

Una de las discusiones doctrinales y jurisprudenciales en cuanto a los datos personales tiene que ver con el consentimiento por parte del individuo, el método de recolección y transmisión de los datos y el acceso a datos de terceros, particularmente en servicios de redes sociales como lo son Facebook o Instagram. La tendencia de muchas legislaciones es exigir un consentimiento claro, afirmativo, libre, expreso, informado, o cualquier otra característica similar, como lo hacen por ejemplo Argentina y Uruguay. Colombia por su parte dispone que autorización es el consentimiento previo, expreso e informado. En Canadá el consentimiento es válido únicamente cuando es razonable suponer que el individuo que lo manifiesta comprende la naturaleza, propósito y consecuencias de la recopilación, uso o divulgación de su información personal.

El RGPD establece que el consentimiento es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. De igual manera el reglamento determina que al momento de analizar si el consentimiento se ha dado de manera libre o no se tomará en cuenta el hecho de si los datos recolectados son necesarios para la ejecución del contrato. En el Reino Unido, siguiendo las disposiciones de la Unión Europea, el consentimiento en relación con el procesamiento de datos personales de un individuo se refiere a una manifestación presentada de manera libre y que se caracteriza por ser específica, informada e inequívoca y mediante la cual el individuo da a conocer mediante una acción afirmativa su aceptación al procesamiento de los datos. La legislación japonesa se encuentra rezagada en la materia ya que no define consentimiento, limitándose a establecer que el mismo debe ser obtenido previamente lo que ha ocasionado discusiones en la doctrina sobre el contenido y necesidad de suplir este vacío legal.

El proyecto de ley adolece de deficiencias graves en cuanto al consentimiento. Una lectura del artículo 6 del proyecto revela que el consentimiento debe ser previo, irrefutable y expreso y que la persona debe ser informada sobre al uso que se le dará de sus datos personales. La redacción de este artículo no establece que tal información sobre el uso debe ser proporcionada previamente al interesado, únicamente que el consentimiento debe ser previo a la recolección. La norma tampoco requiere que el consentimiento sea informado, por lo que nada evita que se obtenga un consentimiento sin informar al titular de la información previamente. También preocupa que el proyecto establezca una excepción para el consentimiento en relación con una categoría de

personas que se limiten a indicar antecedentes tales como la pertenencia de la persona natural a una organización, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento. Tampoco se disponen normas relativas al consentimiento a la recolección de información de menores de edad, situación sobre la cual encontramos reglas en muchas de las legislaciones consultadas.

Si bien la recolección de información personal debe realizarse en base al consentimiento del titular de esta tanto la doctrina comparada como las legislaciones y jurisprudencia son claras en requerir que tal consentimiento sea informado. En Japón por ejemplo, el propósito de uso de los datos debe especificarse lo más posible e inclusive establece que en caso de que el operador de los datos sea parte de una fusión corporativa la nueva entidad no podrá utilizar los datos recolectados para los fines establecidos en la autorización original La normativa japonesa establece claramente que el consentimiento no puede obtenerse por medios fraudulentos y en los casos en los que la información se obtenga como parte de la celebración de un contrato es necesario que el usuario reciba información detallada sobre los propósitos de uso de dicha información. De igual manera, el operador no puede cambiar su política de uso de datos a tal grado que deje de guardar relación con la información proporcionada al individuo al momento en que otorgo su consentimiento.

En caso de que el operador obtenga los datos de un individuo por motivos diferentes a un contrato la ley le impone la obligación de informar al titular de estos sobre el uso que pretenda darle a los datos personales a la mayor brevedad posible. Las legislaciones latinoamericanas se rigen por los principios de información previa y de especificidad en cuanto a la política de uso de los datos personales. Argentina requiere que al momento de obtener el consentimiento se le informe al sujeto la finalidad para la cual serán utilizados los datos y quienes serán los destinatarios o posibles destinatarios, le existencia de registros y bancos de datos, así como la identidad y domicilio del responsable, si las respuestas que el sujeto da son obligatorias o facultativas, las consecuencias de proporcionar o no los datos, y finalmente la facultad del interesado para ejercer sus derechos.

Colombia obliga al responsable del tratamiento de datos a proporcionar al titular de los mismos información relativa a cómo serán procesados sus datos personales, si las respuestas que proporciona son facultativas o no, pero solo en caso en que versen sobre datos de niños y adolescentes. El responsable también debe informar al titular sobre sus derechos y la dirección física y electrónica, así como el teléfono del responsable de los datos.

La ley uruguaya dispone que al momento de recabar información personal es necesario informar previamente de manera expresa, precisa e inequívoca la finalidad que se le dará a los datos, la existencia de una base de datos, así como la identidad y domicilio del responsable, el carácter obligatorio o no del cuestionario, las consecuencias de proporcionar o no la información y finalmente la posibilidad por parte del titular para ejercer sus derechos.

La unión europea por su parte ha ido más allá al establecer que cuando el consentimiento se da dentro del contexto de una declaración escrita que también verse sobre otros asuntos, es necesario que la solicitud de consentimiento sea presentada de manera inteligible y de fácil acceso en un lenguaje claro y sencillo, de tal manera que pueda separarse de otros asuntos dentro del documento. Se considera nula la declaración de uso que vaya en contra de cualquiera de las normas del reglamento. De esta manera la doctrina es clara en que la persona o corporación que recolecta

los datos tiene una serie de obligaciones que nacen aun antes de que comience su tarea de recopilación. Sin embargo, el proyecto de ley guarda silencio al respecto, limitándose a establecer en su artículo 24 del proyecto que cuando la recolección de datos se realice por medios digitales o la internet las obligaciones establecidas en el proyecto serán complementadas por las "políticas de privacidad" y/o "Condiciones de Servicio". Consideramos que tal referencia a un documento privado como lo son las condiciones de servicio de una aplicación o página virtual para complementar las obligaciones del operador va en contra del fin del proyecto y la tendencia actual en el derecho comparado.

En cambio, el proyecto de ley panameño no desarrolla políticas ni reglas en cuanto al uso, propósito, naturaleza, etc. en tema de tratamiento de datos. El artículo 5 decreta que el titular tiene derecho a que sus datos no sean utilizados para fines distintos de los que haya sido informado y le otorga el derecho de oponerse a usos no autorizados.

El artículo 10 escuetamente establece que los datos personales deben utilizarse para los fines determinados, explícitos y lícitos para los cuales hubieren sido autorizados al momento de su recolección sin especificar la manera en que tal información debe ser proporcionada al usuario. Esta información es de fundamental importancia para el usuario final quien debe considerarla al momento de tomar la decisión sobre sí autoriza o no el tratamiento de su información. La ley tampoco establece si tal información relativa al uso de los datos personales debe proporcionarse de manera independiente o puede ser parte de un contrato. El artículo 5 del proyecto dispone que la información recopilada solo puede ser utilizada para los fines que expresamente informados al titular, pudiendo este último oponerse a usos sobre los cuales no haya sido informado aparte de cualquier responsabilidad civil o penal que pudiera existir. El mismo artículo impone la obligación de informar sobre la no obligatoriedad de las preguntas en casos de encuestas, estudios de mercado, sondeos de opinión pública y otros instrumentos semejantes. Seguidamente el artículo 6 requiere que se informe debidamente al titular sobre el uso que se les dará a sus datos personales. El artículo 13 le otorga al titular de los datos personales los derechos de acceso, rectificación, cancelación y oposición, pero no contempla ningún tipo de derecho, a la información. En específico, el proyecto guarda silencio sobre cuándo debe informarse al titular de los datos o los requisitos que debe cumplir la política de uso de los datos.

CONCLUSIONES

Varios sectores de la sociedad claman por la aprobación del Proyecto de Ley No. 463 de protección de datos de carácter personal como una manera de que nuestro país se adecue a estándares internacionales y así impulsar nuestra competitividad. Sin embargo, no podemos compartir esta opinión. Somos conscientes de que Panamá se encuentra rezagada en esta materia y que los requerimientos de una sociedad informática nos obligan a adaptarnos a las nuevas tecnologías para poder proteger los derechos tanto de nacionales como extranjeros. No obstante, consideramos que la adopción de este proyecto de ley no se traducirá en un desarrollo positivo para el país en materia de protección de datos. En primer lugar, la falta de principios rectores claramente delineados limita mucho la eficacia del proyecto de ley. Aunado a esto tenemos el hecho de que el proyecto hace referencia en varias ocasiones a leyes especiales; otorgándoles preferencia sobre las normas contenidas en el mismo.

La principal función de una ley de protección de datos es crear un marco común para que las entidades tanto públicas como privadas tengan una guía al momento de recolectar, procesar, transmitir y, en caso de ser necesario divulgar datos personales, principios que se convierten en la base sobre la cual se desarrolla la política informática de un país. Estos principios generales los encontramos aun en países federalistas como Estados Unidos aun cuando las reglas para cada tipo de información se encuentren consagradas en leyes especiales. Si lo que se desea es seguir un modelo similar al estadounidense, lo ideal sería incluir los principios rectores de la protección de datos personales en este proyecto y que la interpretación y aplicación de las leyes especiales se de en base a los mismos. Por otra parte, no comprendemos qué se pretende al permitir que las políticas de uso de cada operador sirvan como complemento para normas cuya función es proteger los datos personales de los individuos, sobre todo si se toma en cuenta la falta de principios generales. Las experiencias modernas con servicios de redes sociales y aplicaciones similares demuestran que dejar tales decisiones a actores privados no resulta en una protección adecuada de los derechos de los usuarios.

En segundo lugar, nos parecen peligrosas algunas excepciones establecidas en el proyecto. Por ejemplo, el proyecto dispone que las normas no serán aplicables a la información obtenida mediante un proceso previo de disociación. Sin embargo, no queda claro si se requiere el consentimiento del titular de la información al momento de recolectarla, aun cuando esta sea sometida al proceso de disociación posteriormente. La ley también dispone que no se requiere consentimiento para el tratamiento de la dirección y fecha de nacimiento del individuo, ya que en la práctica de muchas instituciones financieras y otros servicios esta información es usada para confirmar la identidad del usuario al acceder a servicios en línea o vía telefónica. La redacción del proyecto revela que el mismo no se adapta a las realidades de la era informática ya que muchas normas parecen redactadas sin tomar en cuenta las características de una sociedad conectada 24 horas al día. No comprendemos por que la información sobre la obligatoriedad de responder o no a preguntas se limite únicamente a ciertos tipos de recolección de datos. Tampoco se abordan temas como la recolección de datos personales de manera pasiva producto de contactos en las redes sociales o derechos sobre información genética o biométrica.

En conclusión, tomando en cuenta los compromisos internacionales de Panamá en materia de protección de derechos humanos y las tendencias modernas en el derecho comparado, en particular el requerimiento que el RGPD hace para el intercambio de información consideramos que es necesario comenzar nuevamente desde cero, tomando en cuenta los últimos avances jurídicos en la materia.

BIBLIOGRAFÍA

BBC. *Cambridge Analytica: The story so far.* (En línea) (Fecha de consulta: 3 de septiembre de 2018). Disponible en: https://www.bbc.co.uk/news/technology-43465968

BENNETT, Collin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Casa editorial: Cornell University Press, Primera edición, 1992.

CATE, Fred H., CULLEN, Peter, MAYER-SCHONBERGER, *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* (2014) (En línea) (Fecha de acceso: 3 de septiembre de 2018)

Disponible en: https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf

GREENLEAF, Graham *Global Data Privacy Laws: Forty Years of Acceleration,* Privacy Laws and Business International Report, No. 112, pp. 11-17 (2011)

GREENLEAF, Graham. *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, including Indonesia and Turkey, 2017)* 145 Privacy Laws & Business International Report, pp. 10-13 (2017)

GUTWIRTH, Serge, POULLET, Yves, DE HERT, Paul, LEENES, Ronald. *Computers, Privacy and Data Protection: an Element of Choice.* Casa editorial: Spinger. Edición 2011.

HUFFINGTON POST. *How Google Is Changing The Way We Think* (2015) (En línea) Inglaterra (Fecha de acceso: 3 de septiembre de 2018) Disponible en: https://www.huffingtonpost.com/entry/google-changes-thinking_us_55dc8069e4b04ae497046fa6

INFORMATION COMMISIONER´S OFFICE. *Investigation into the use of data analytics in political campaigns.* (En línea) Inglaterra. (Fecha de consulta: 3 de septiembre de 2018) Disponible en: https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

NEW YORK TIMES, *La empresa que explotó millones de datos de usuarios de Facebook.* (En línea) New York. (Fecha de consulta: 3 de septiembre de 2018) Disponible en: https://www.nytimes.com/es/2018/03/20/cambridge-analytica-facebook/

OECD, *The OECD Privacy Framework* (2013). (En línea) (Fecha de acceso: 3 de septiembre de 2018) Disponible en: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

ROSENDAAL, Arnold. *Facebook tracks and traces everyone: Like this!*. Tilburg Law School Legal Studies Research Paper Series No. 03/2011

RUBINSTEIN, Ira S. *Big Data: The End of Privacy or a New Beginning?* International Data Privacy Law, Vol. 3 No.2 pp. 74-87 (2013)

SCIENTIFIC AMERICAN. *The Internet Has Become the External Hard Drive for Our Memories* (2013) (En línea) (Fecha de acceso: 3 de septiembre de 2018) Disponible en: https://www.scientificamerican.com/article/the-internet-has-become-the-external-hard-drive-for-our-memories/

SCHÜNEMANN, Wolf J., BAUMANN, Max-Otto (EDS.). *Privacy, Data Protection and Cybersecurity in Europe***.** Casa editorial: Springer, Primera edición 2017.

TENE, Omer, POLONETSKY, Jules. *Big Data for All: Privacy and User Control in the Age of Analytics.* Northwestern Journal of Technology and Intellectual Property, Vol. 11 pp. 239-273 (2013)

THE OBSERVER. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.* (En línea) Inglaterra. (Fecha de consulta: 3 de septiembre de 2018) Disponible en: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

LEYES

Argentina	Ley No. 25236 de 2000
Canadá	Personal Information Protection and Electronic Documents Act
Estados Unidos	Privacy Act de 1974 (5 U.S.C. § 552a)
Colombia	Ley Estatuaria 1581 de 2012
Japón	Ley No. 57 de 2003
Reino Unido	Data Processing Act de 2018
Reglamento (Ue) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016	
Uruguay	Ley 18331 de 2008

Artículo recibido: 14 de septiembre de 2018

Aprobado: 26 de septiembre de 2018