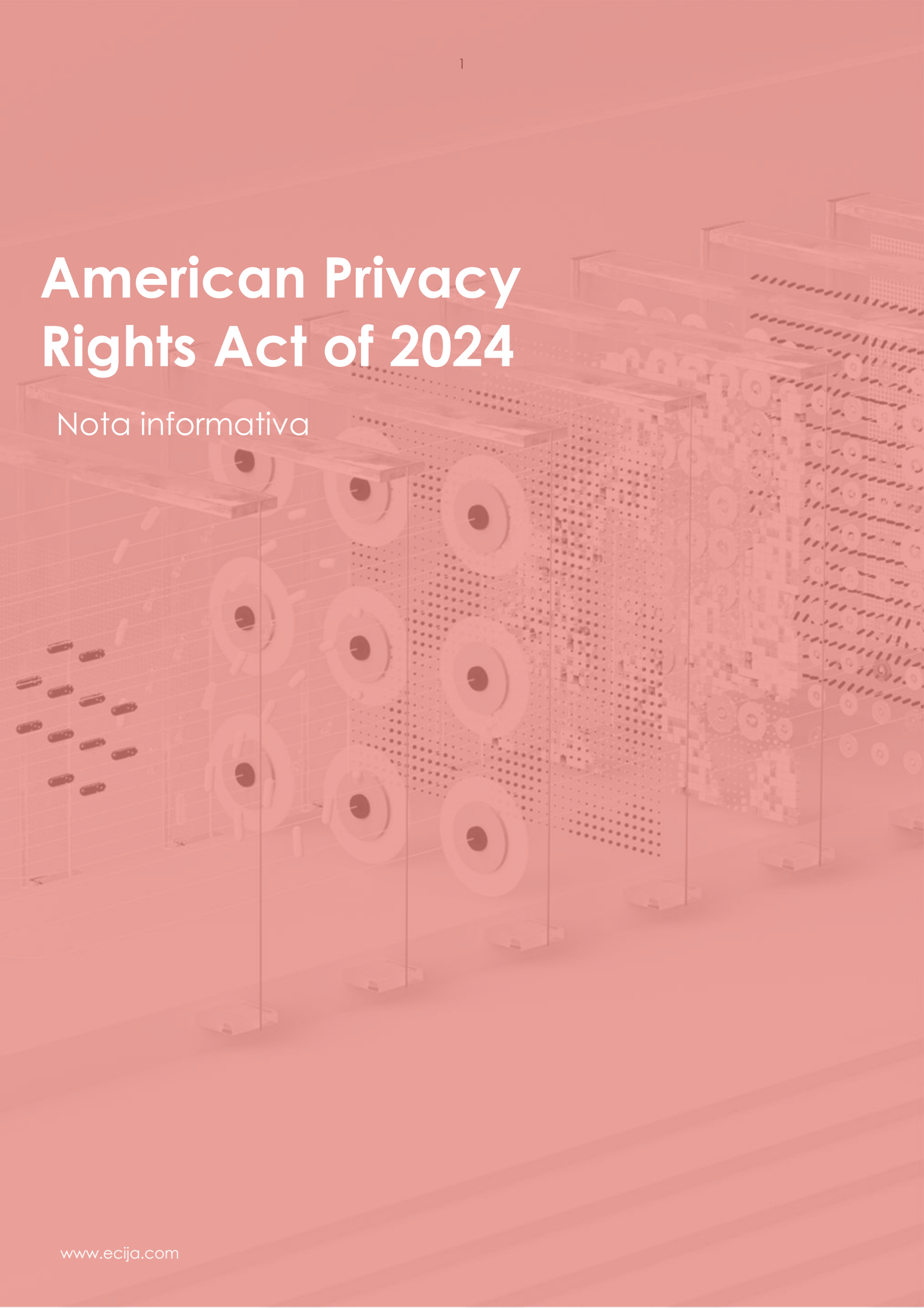
American Privacy Rights Act of 2024

Nota informativa



El primer borrador de la American Privacy Rights Act of 2024 ("APRA"), presentado recientemente, podría convertirse en la primera Ley Federal para la protección de la privacidad y la seguridad de los datos de los ciudadanos estadounidenses, lo que supone un cambio de paradigma en la concepción de la protección de datos personales en el país, evolucionando desde la tradicional autorregulación voluntaria hacia el establecimiento de obligaciones específicas, mucho más cercano al modelo europeo.

De hecho, el texto recoge algunos aspectos similares a la normativa europea, incorporando conceptos tanto del Reglamento General de Protección de Datos, mediante ciertas obligaciones similares para el tratamiento de datos personales, como del Reglamento de Servicios Digitales (DSA), estableciendo deberes específicos para los *"Large Data Holder"*.

Principales consideraciones del APRA:

Alcance y ámbito de aplicación

El APRA establece un marco regulatorio que limita su aplicación a entidades que tienen un papel determinante en el tratamiento, recolección, conservación o transferencia de datos, y que cumplen con ciertos criterios legales, como estar sometidas a la jurisdicción de la Comisión Federal de Comercio (en adelante, "**FTC**"), equiparándose, de forma simplificada, a aquellas entidades que ofrecen productos o servicios a consumidores.

Minimización de datos

El APRA regula la minimización de datos de forma parecida al RGPD. En este sentido, las entidades afectadas por el APRA, así como los proveedores de servicios que operen en su nombre, no podrán tratar, recabar o enviar datos cuando no sea necesario, proporcional o limitado a proveer un producto o mantener un servicio solicitado por un interesado o, en su caso, para proveer comunicaciones que puedan ser previstas de forma razonable en el contexto de una relación o con una finalidad permitida por la misma ley. La FTC podrá emitir directrices sobre lo que se considerará "razonablemente necesario y proporcional", de acuerdo con el principio de minimización de datos recogidos en el APRA.

Legitimación en el tratamiento de datos

A diferencia del RGPD, el APRA no se fundamenta en "bases de legitimación", sino en quince finalidades específicas para el tratamiento de datos, incluyendo el cumplimiento de una obligación legal, la seguridad pública o la prevención de fraude, entre otros. Así, de un modo más práctico y directo que el RGPD, el APRA cubre un rango amplio de finalidades para el tratamiento de datos, escapando de la diferenciación (y a veces confusión) europea entre legitimación y finalidad del tratamiento. En este sentido, los datos sensibles (incluidos aquí los biométricos) podrán ser tratados con el único límite en el consentimiento expreso de los sujetos afectados.

Transparencia y derechos de los interesados

El APRA requiere que las entidades y los proveedores de servicios publiquen políticas de privacidad que garanticen un nivel de transparencia similar al establecido en el RGPD. Esto incluye informar sobre los derechos de los interesados y ofrecer información en todos los idiomas en los que se ofrecen productos o servicios, asegurando a su vez la posibilidad de retirar el consentimiento una vez otorgado.

Las políticas deberán recoger los derechos de acceso, rectificación, supresión y la portabilidad de los datos, y las entidades deberán responder a su solicitud en un plazo no superior a 30 días naturales, como norma general.

Para dar cumplimiento con este principio de transparencia, las políticas de privacidad deberán estar actualizadas y contener información sobre la identidad de la empresa, las categorías de datos recopilados, los fines del tratamiento, los destinatarios de los datos (incluidos proveedores de servicios y terceros), los plazos de conservación de los datos, las medidas de seguridad establecidas por éstos y la fecha de entrada en vigor de la política de privacidad

Datos sensibles

Los "datos sensibles" en el APRA, son similares a la categoría de datos especiales del artículo 9 del RGPD. No obstante, en general, es posible tratar los datos sensibles que no se refieran a datos biométricos o genéticos siempre que cumpla una de las 15 finalidades que estipula la ley. Los datos biométricos y genéticos requerirán siempre consentimiento para su tratamiento salvo en tasadas excepciones. Por su lado, las transferencias de datos sensibles, en cualquier caso, requerirán del consentimiento expreso del individuo para su licitud.

Así, en el APRA, los datos sensibles son:

- Identificadores gubernamentales privados como números de seguro social.
- Datos médicos o de salud mental de individuos, incluyendo el tratamiento.
- Información genética, datos biométricos o de geolocalización precisa.
- Números de cuentas financieras o tarjetas de crédito.
- Comunicaciones privadas como correos electrónicos o mensajes de texto.
- Credenciales de acceso a cuentas o dispositivos.
- Información sobre el comportamiento o la privacidad sexual de un individuo.
- Las comunicaciones privadas de un individuo, así como información relacionada con los detalles de las llamadas, a menos que la entidad afectada sea el destinatario previsto de la comunicación. También el calendario y el contenido multimedia creado para uso privado.
- Datos sobre actividades en línea y uso de servicios de video.
- Información sobre la raza, etnia, religión, sexo o país de origen.
- Datos relacionados con menores (en el APRA, menores de 17 años).

Oficial de privacidad

De acuerdo con lo establecido en el APRA, las entidades afectadas por la norma deberán designar o un oficial de privacidad (similar a un DPO del RGPD) o un oficial de seguridad de la información, que deberá ser un empleado cualificado para el cargo dentro de la organización. Estos oficiales deberán implementar programas de privacidad y seguridad de los datos y garantizar así el cumplimiento continuo de la ley, como por ejemplo el establecimiento de procedimientos ante violaciones de seguridad.

Evaluaciones de impacto

Se prevé la realización de Evaluaciones de impacto obligatorias para las entidades catalogadas como "*Large Data Holder*". Esta obligación se aplica por el tipo de responsable y no por el nivel de riesgo de los tratamientos. Sin embargo, no se ofrecen pautas concretas de cómo realizar estas evaluaciones de impacto, más allá de consideraciones generales, por lo que quedará en manos de las organizaciones el desarrollo de este tipo de procedimientos.

Data Brokers

A lo largo del APRA se recogen a su vez estipulaciones sobre los intermediarios de datos ("***Data Brokers***"). A estos efectos, los *Data Broker* son una figura con similitudes con el encargado de tratamiento definido en el RGPD, pero que presenta sus propias particularidades. El APRA, define a los *Data Brokers* como aquellas entidades cuya principal fuente de ingresos proviene del tratamiento o transferencia de datos que la entidad no recopiló directamente de los propios individuos.

De esta forma, la principal fuente de ingresos es aquellos que constituyen más del 50% de todos los ingresos de la entidad durante un período de 12 meses, o los ingresos obtenidos a partir del tratamiento o transferencia de datos de más de 5.000.000 de individuos cuyos datos no fueron recolectados directamente por la entidad.

Transferencias internacionales de datos personales

En cuanto a las transferencias internacionales de datos en el sentido en el que se entienden en Europa, como aquellas realizadas fuera de un determinado territorio, no están previstas de forma específica en el APRA. A estos efectos, si bien es cierto que existen ciertas obligaciones en la cesión de datos, cualquier cesión de datos realizada dentro o fuera de los EE. UU goza de los mismos límites y obligaciones.

Large Data Holder

Como mencionábamos con anterioridad, el APRA contiene algunas obligaciones específicas para los *Large Data Holder* o, en su traducción en español, Grandes tenedores de datos (de forma similar a la DSA). A estos efectos, se refiere a una entidad afectada por la normativa o proveedor de servicios que, en el año anterior, tuvo ingresos anuales de al menos $250.000.000 y recopiló, trató o conservó cantidades de datos de al menos:

- Datos de 5.000.000 individuos, además de 15.000.000 dispositivos portátiles que puedan identificar al menos a un individuo y 35.000.000 dispositivos conectados que igualmente pudieran identificar al menos a un individuo;
- O, en caso de que los datos fueran considerados sensibles, Datos de 200.000 individuos, además de 300.000 dispositivos portátiles que puedan identificar al menos a un individuo y 700.000 dispositivos conectados que igualmente pudieran identificar al menos a un individuo.

Algunas de las obligaciones específicas de este tipo de entidades son:

- La obligación de publicar sus políticas de privacidad aplicables en los últimos 10 años. Además, ofrecer en su web una primera capa informativa (similar al *banner* de cookies) con los puntos esenciales del tratamiento de datos y con una extensión no superior a las 500 palabras.
- Presentar certificaciones anuales a la FTC sobre sus controles internos y oficiales.

- Realizar evaluaciones de impacto en la privacidad de los datos cada dos años, considerando el uso de tecnologías emergentes para la protección de los datos.
- Plazo de 15 días para responder a una solicitud de ejercicio de derechos.
- Deben tener tanto Oficial de protección de datos como de seguridad de la información.

Régimen sancionador

Respecto a las sanciones recogidas en el APRA, se estipulan sanciones por incumplimiento desde los 100$ diarios, hasta un límite de 10.000$ anuales para algunas infracciones concretas (ausencia de registro de los "*Data Brokers*"), así como un límite indefinido en relación con el "daño real" causado mediante cualquier infracción del APRA. Estas sanciones difieren en gran medida a las establecidas expresamente en el RGPD, que tipifica sanciones de hasta 20 millones de euros o el 4% de la facturación anual global de la empresa infractora.

A este respecto, como en la mayoría de las leyes estadounidenses, habrá que esperar a la concreta aplicación de la ley en los tribunales para poder saber de forma aproximada las cuantías a las que se enfrentarán los infractores.

Conclusión

El American Privacy Rights Act of 2024 representa un paso significativo hacia la protección de la privacidad y los datos personales de los individuos en un entorno cada vez más digitalizado.

En un mundo donde los riesgos para la privacidad y la seguridad de los datos son una realidad, el APRA ofrece un marco legal más sólido que contribuirá a crear un entorno digital más seguro y confiable para todos los estadounidenses, sobre todo teniendo en cuenta que únicamente unos pocos Estados contaban con normativa relativa a la protección de datos en este país. Así, el APRA supondría una Ley Federal, superior en rango a cualquier otra estatal aprobada con anterioridad, como la Ley de California, equiparando el nivel de exigencia de ciertas obligaciones para aquellas empresas afectadas por la norma de cualquier Estado del país americano, sin perjuicio de que cada Estado pueda desarrollar la normativa a posteriori.

El alcance del APRA no es total, centrándose sobre todo en la defensa de los consumidores, pero si muy relevante para Europa. En este sentido, muchas de las entidades que prestan servicios transfronterizos entrarían dentro de la categoría de *Large Data Holders* y, por tanto, estarían más cercanas al cumplimiento de los estándares europeos de protección de datos, lo que puede facilitar la contratación de sus servicios sin que ello suponga un riesgo adicional como ocurre actualmente.

No obstante, el texto se encuentra aún sujeto a cambios y habrá que esperar a su promulgación definitiva y al desarrollo posterior que realicen por su parte el FTC y los tribunales estadounidenses, para poder analizar el marco regulatorio completo que ofrecerá entonces EE. UU en relación con la protección y la seguridad de los datos.

Calle Serrano, 69.
28006 Madrid
www.ecija.com

Área de Protección de Datos de ECIJA
info@ecija.com
Telf: + 34 91.781.61.60