V. PROTECCIÓN DE DATOS PERSONALES EN LA INDUSTRIA DEL JUEGO

1. *México*

Una de las adecuaciones normativas recientes en nuestro país es la introducción de la protección de datos personales para las entidades productivas particulares. El sector privado nacional enfrenta un reto considerable en la materia. Las características del modelo de protección de la información personal en México hacen que el cuidado y la responsabilidad que conlleva el trabajo con datos de los individuos sea una carga jurídica, administrativa y económica de importancia mayor. Para la industria del juego con apuestas y sorteos no hay excepción.

A diferencia de otros modelos en el derecho comparado, la protección de datos personales se ha introducido a nuestro país como un derecho fundamental. Lo anterior tiene consecuencias importantes para los operadores económicos, ahora subordinados a la normatividad de esta materia. Quizá la de mayor trascendencia es que, contra el entendido tradicional, los sujetos privados ahora son potenciales violadores de derechos humanos. Ésta es una novedosa característica en nuestro sistema jurídico, ya que la materia de datos personales fue pionera en el modelo que seguirían luego el juicio de amparo y el acceso a la información pública. Al mismo tiempo, el sistema jurídico mexicano ha tomado una nueva ruta hacia la protección integral de los derechos humanos desde 2011.

Del punto anterior se deriva que la protección de datos se haya distinguido de los derechos de los consumidores e incluso de la normatividad laboral. La protección de datos se erige como un área robusta e integral de protección de un derecho fundamental con un entramado normativo que regula transversalmente todos los procesos administra-

tivos y económicos que involucren información personal de manera taxativa; medidas de cuidado particulares; medios de verificación; importantes sanciones administrativas y económicas, así como la presencia de un órgano especializado para el seguimiento de la implementación de la nueva normatividad, su verificación y posible sanción.

A grandes rasgos, podríamos afirmar que en el derecho fundamental a la protección de datos personales convergen dos tipos de actividades para los responsables, en este caso: los permisionarios y operadores de salas de sorteos de números o símbolos, y centros de apuestas remotas. Las primeras se refieren a las actividades administrativas y organizacionales que se desprenden de los axiomas rectores de la protección de datos personales, que son los principios de: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. Aunado a dichas actividades, los permisionarios y operadores de salas de sorteos de números o símbolos y centros de apuestas remotas deben garantizar el ejercicio de cuatro derechos consagrados en el texto de la Constitución federal: los derechos de acceso, rectificación, cancelación y de oposición (derechos ARCO).

Las primeras actividades dan cuenta de las medidas de cumplimiento orientado por los principios rectores. Algunos ejemplos de éstas son la obtención del consentimiento al momento de recabar datos; el cumplimiento del principio de información a través del aviso de privacidad; el establecimiento de mecanismos administrativos idóneos para la selección de los datos estrictamente necesarios y oportunos; el uso respetuoso de la información de los clientes y empleados; el establecimiento de medidas preventivas para la protección de la información, etcétera.

En contraste, las segundas están orientadas a dar a los titulares, es decir, a los dueños de la información, la garantía de poder acceder, rectificar, cancelar y oponerse al uso ilegítimo de su información. De éstas vale la pena señalar el establecimiento de un departamento o encargado de dar respuesta y seguimiento a las solicitudes; el mapeo y establecimiento de procedimientos internos para potenciar las respuestas oportunas; la capacitación del personal para el posible litigio frente a los procedimientos ante las autoridades competentes, entre otras.

El último tema relevante es el entramado institucional que se ha instaurado para la protección de los datos personales a nivel nacional, que conlleva una serie de procedimientos administrativos y su sustanciación

ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Los procedimientos derivados de la ley son el de verificación, de protección de derechos y el de imposición de sanciones. El primero da cuenta del mecanismo con el que cuenta la autoridad para verificar el cumplimiento de la normatividad; el segundo, para revisar el debido ejercicio de los derechos ARCO, y el último impone sanciones ante el incumplimiento constatado en alguno de los anteriores.

Como se puede ver, las cargas jurídicas y administrativas para los permisionarios y operadores son un hecho, y las deben cumplir. Lo anterior puede generar riesgos económicos derivados de las sanciones por incumplimiento, que van de la amonestación a la multa de más de 128 mil unidades de medida y actualización (UMA),[100] equivalentes —al día en que se escriben estas líneas— a más de 90 millones de pesos. Solamente para el primer semestre de 2016, el INAI ha impuesto multas que superan los 50 millones de pesos.[101] Aunado a lo anterior, la relevancia que el tema va tomando entre los individuos hace que una infracción hecha pública redunde en descrédito a nivel nacional e internacional de las organizaciones.

El modelo de análisis que se propone parte de la necesidad práctica de los sujetos regulados para dar cumplimiento a las normas en la materia. En este sentido, se propone una estructura que permita delinear claramente los principales retos en la protección debida de los datos personales de los titulares de éstos. Así las cosas, se analizan los principios y derechos centrales. Al mismo tiempo, se enumeran las principales obligaciones, las potenciales sanciones, así como algunas medidas de prevención de las eventualidades expuestas en los anexos correspondientes.

A. *Los permisionarios y operadores*

Como punto de partida de este apartado es necesario despejar una primera cuestión: ¿son los permisionarios y operadores de salas de sor-

[100] El cálculo se hace tomando en consideración la multa mayor establecida de 320 mil días de salario, una posible multa adicional de la misma cantidad y, llevando al extremo el ejemplo, las modalidades de sanción para datos sensibles.

[101] Instituto Nacional de Acceso a la Información y Protección de Datos, Boletín INAI/206/16, 24 de julio de 2016.

teos de números o símbolos y centros de apuestas remotas sujetos obligados de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares? La respuesta es sí. Lo anterior descansa en el siguiente argumento:

La LFPDPPP establece que los sujetos regulados por la misma son los particulares, sean personas físicas o morales, de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

— Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
— Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial (artículo 2o., LFPDPPP).

Como señala el ordenamiento, es aplicable la normatividad a cualquier persona física o moral que lleve a cabo el tratamiento de datos personales. En este sentido (aunque será desarrollado a profundidad más adelante), el mismo ordenamiento define en su artículo 3o. qué se debe entender por tratamiento de datos personales: "La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales" (artículo 3o., LFPDPPP).

Siguiendo la idea planteada, los permisionarios y operadores son definidos en el RLFJS de la siguiente manera:

— Operador: sociedad mercantil con la cual el permisionario puede contratar o asociarse para explotar su permiso, en términos de lo dispuesto en el RLFJS.
— Permisionario: persona física o moral a quien la SEGOB otorga un permiso para llevar a cabo alguna actividad en materia de juegos con apuestas y sorteos permitida por la LFJS y el presente RLFJS (artículo 3o., RLFJS).

En una lectura simple, ambas figuras quedan comprendidas en el ámbito de "las personas físicas o morales". Lo anterior despeja las dudas del ámbito de aplicación subjetiva de la norma en comentario.

Ahora bien, la siguiente cuestión a desarrollar es si los permisionarios y operadores llevan a cabo tratamiento de datos de carácter personal. Sobre este punto es dable hacer notar que, desde el punto de vista reglamentario, tanto operadores como permisionarios recaban, almacenan y transmiten datos personales, y este simple hecho los convierte en sujetos que tratan información personal. Muestra de ello son las siguientes obligaciones ante las autoridades reguladoras de los juegos con apuestas y sorteos que se desprenden del RLFJS.

De conformidad con el artículo 85, los establecimientos deben registrar el número de cuenta y la identidad del apostador cuando capten apuestas vía internet, telefónica o electrónica.

> Artículo 85. Los establecimientos podrán captar apuestas vía internet, telefónica o electrónica. Para ello, deberán establecer un sistema de control interno para las transacciones que se efectúen por estas vías, elaborando por escrito la descripción de los procedimientos y reglas que aseguren la inviolabilidad e impidan la manipulación de los sistemas de apuestas. En dicho sistema deberá quedar registrado, al menos:
>
> I. El número de la cuenta e identidad del apostador, y
>
> II. La fecha, hora, número de la transacción, cantidad apostada y selección solicitada.
>
> La mecánica de captación de apuestas deberá ser aprobada previamente por la Secretaría.

En términos del artículo 86 del RLFJS, los establecimientos pueden tener acceso a los datos de las cuentas bancarias de los usuarios, cuando capten apuestas vía internet, telefónica o electrónica.

> Artículo 86. Sólo se captarán o cruzarán apuestas en efectivo, salvo aquellas que se ejecuten vía internet, telefónica o electrónica, las cuales se entenderán como pagadas cuando por esta misma vía se realice la confirmación de pago por la institución bancaria correspondiente, ya sea al apostador o al permisionario.

De conformidad con el artículo 87, las apuestas vía telefónica deben quedar grabadas en un registro de audio.

> Artículo 87. Los permisionarios y operadores a que se refiere este capítulo deberán cumplir con el siguiente procedimiento para la expedición de los comprobantes de apuesta:
>
> …
>
> II. En las apuestas vía internet, telefónica o electrónica no se emitirá boleto alguno, pero la información de dicha apuesta quedará registrada en el sistema central de apuestas inmediatamente después de haber pagado la apuesta. Tratándose de apuestas vía internet o electrónica, los participantes deberán tener acceso, para consulta e impresión, a una constancia de su número de folio y de los derechos que les correspondan. Las apuestas vía telefónica, previo consentimiento del apostador, deberán quedar grabadas en un registro de audio;
>
> …

Los artículos 88 y 89 establecen que los permisionarios y operadores deben conservar la información mediante la cual se determinen los comprobantes ganadores, así como los propios comprobantes ganadores. Se trata, en ambos casos, de documentación que eventualmente puede contener datos personales de los ganadores.

> Artículo 88. Los permisionarios deberán cumplir el siguiente procedimiento para el pago de premios:
>
> …
>
> IV. La información oficial mediante la cual se determinen los comprobantes ganadores, deberá ser conservada por el permisionario durante los 90 días hábiles siguientes a la celebración del evento, y
>
> …
>
> Artículo 89. El permisionario deberá resguardar el registro de los comprobantes ganadores cobrados durante 90 días hábiles, con el fin de aclarar cualquier duda o inconformidad que sea presentada ante las autoridades correspondientes.

En términos del artículo 134, cuando acontezcan disputas entre el organizador y los participantes, el permisionario deberá tomar conocimiento de la situación, de modo que es posible que tenga acceso a los datos personales de los quejosos.

> Artículo 134. En caso de disputas entre el organizador y los participantes, el representante del permisionario deberá tomar conocimiento de la situación y proveer al quejoso la información disponible, incluyendo la contenida en el texto del permiso otorgado por la Secretaría, a efecto de que, en su caso, haga valer las acciones que estime conducentes.

De acuerdo con los artículos 44 y 45, los permisionarios y operadores tienen datos personales de las personas físicas que prestan servicios profesionales vinculados al corretaje, cruce de apuestas o intendencia de frontón y sus supervisores en un establecimiento autorizado, como su edad, nacionalidad, calidad migratoria, antecedentes profesionales y antecedentes penales. A este respecto, hay que advertir que si bien no se trata de datos personales de los clientes, sí es información de particulares que prestan servicios a los de salas de sorteos de números o símbolos y centros de apuestas remotas:

> Artículo 44. Para que una persona física pueda prestar sus servicios profesionales vinculados al corretaje, cruce de apuestas o intendencia de frontón en un establecimiento autorizado, deberá cumplir con los siguientes requisitos:
>
> I. Ser mayor de edad;
>
> II. Acreditar la nacionalidad mexicana y, en caso de ser extranjero, su legal estancia en el país y el permiso de las autoridades migratorias para desempeñar las actividades para las que sea contratado;
>
> III. Comprobar con medios documentales o técnicos que cuenta con los conocimientos técnicos o profesionales suficientes para realizar la actividad respectiva de manera eficiente;
>
> IV. No haber sido condenado por delito intencional de índole patrimonial, fiscal o relacionado con el crimen organizado o de operaciones con recursos de procedencia ilícita;
>
> V. Los supervisores de apuestas, jefes de sala e intendentes de frontón deberán otorgar al permisionario una fianza para asegurar el debido cumplimiento de su función, y
>
> VI. Aportar y actualizar la información que sea necesaria para integrar la Base de Datos prevista en el artículo 17 del presente Reglamento.
>
> Artículo 45. Respecto a los corredores de apuestas, intendentes de frontón y sus supervisores, el permisionario deberá:

I. Recabar la información y abrir un expediente por corredor, con una copia de la documentación e información requerida en el artículo anterior de este Reglamento;

II. Instrumentar los medios necesarios para asegurar que el corredor de apuestas se encuentre debidamente identificado ante el público asistente, mediante el uso adecuado y visible de un gafete, credencial o distintivo similar, y

III. Informar a la Secretaría, por conducto del inspector, cualquier irregularidad o falta en que hubiere incurrido un corredor de apuestas o supervisor de éste.

Por otro lado, es de tener en consideración otra gran cantidad de normas técnicas aplicables a los contribuyentes que en forma habitual realizan juegos con apuestas y sorteos, que los constriñen a proporcionar al SAT la información de los trabajadores en las unidades económicas, así como la información recabada por la naturaleza de las operaciones de cruce de apuestas, sorteos, vigilancia, etcétera.

En resumen, los operadores y permisionarios llevan a cabo diversas actividades que configuran el tratamiento de datos de carácter personal.

La única incógnita hasta este punto es determinar si los operadores y permisionarios pueden ser considerados en alguna de las excepciones establecidas en el propio artículo 2o. de la LFPDPPP.

La norma en comentario señala como posibles excepciones dos supuestos bastante concretos y definidos: en primer lugar se señala a las sociedades de información crediticia, y en segundo término a las personas físicas que posean y usen la información de los individuos con motivos exclusivamente personales, sin fines de divulgación o utilización comercial. En contraste, las actividades naturales de los operadores de salas de sorteos de números o símbolos y centros de apuestas remotas no se pueden acercar conceptualmente a estos supuestos de exclusión, ya que no forman parte del universo de las sociedades de información crediticia al que hace referencia la Ley para Regular las Sociedades

de Información Crediticia (LRSIC). Desde otro punto de vista, tampoco son personas físicas que apliquen un uso personal a los datos; al contrario, la utilización comercial y el cumplimiento de obligaciones jurídicas son las finalidades para las que la requieren los operadores y permisionarios, y éstas son distintas a las personales contempladas en la LFPDPPP.

B. *Definiciones*

Una vez acreditada la aplicación de la normatividad regulatoria en materia de datos personales, es momento de plantear algunas definiciones y conceptos útiles en el entendimiento de la materia. Así las cosas, y en un afán de claridad, se propone entender el tema partiendo de un concepto no desarrollado en la norma, pero que se sugiere definir para delimitar los sujetos, los objetos y la manera en que se relacionan estos elementos: la relación jurídica en el tratamiento de datos personales.

a. La relación jurídica en el tratamiento de datos personales

Entendemos a la relación jurídica en el tratamiento de datos personales como el vínculo que se presenta entre dos sujetos principales, un sujeto activo y un sujeto pasivo, en el que el primero lleva a cabo ciertas actividades respecto a la información personal del segundo. Ahora bien, los sujetos son denominados en la normatividad como el responsable (sujeto activo) y el titular (sujeto pasivo). El objeto de la relación se identifica con el tratamiento o actividad que el responsable lleva a cabo sobre los datos personales (que fungen como el objeto indirecto haciendo un símil con la teoría clásica de las obligaciones).

b. Los datos personales

Ahora bien, es preciso alterar el orden de la definición anterior y partir de la conceptualización del "dato personal" para presentar de

una manera más ordenada los siguientes conceptos. Así las cosas, la LFPDPPP establece qué se entenderá por dato personal: "cualquier información concerniente a una persona física identificada o identificable". Lo anterior implica cuatro elementos: "cualquier información", "una persona física", "concerniente" e "identificada o identificable"; estas últimas dos, características de las primeras. En este sentido se ha pronunciado el Grupo de Trabajo del Artículo 29,[102] autoridad especializada en la materia en la Unión Europea (UE), señalando en su dictamen 4/2007 que el concepto de datos personales se compone por los mismos cuatro elementos (artículo 3o., LFPDPPP).

Por información entendemos, como señala el *Diccionario del Español de México*, el conjunto de datos y conocimientos acerca de algo, es decir, aquello que se conoce sobre un objeto determinado.[103] En relación con este elemento, el dictamen 4/2007 señala:

> …
>
> El primer componente "toda información" sugiere una interpretación lata del concepto, independientemente de la naturaleza o del contenido de la información y del soporte técnico en el que se presente. Esto significa que tanto la información objetiva como la subjetiva sobre una persona, cualquiera que sea su amplitud, y con independencia del soporte técnico que la contenga, puede considerarse como "datos personales"…[104]

Ahora bien, por lo que hace a la relación que debe mantener la información "concerniente" al sujeto es importante. Decimos que cierta información corresponde a una persona cuando señala algún aspecto de

[102] Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la Unión Europea, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

[103] Colegio de México, *Diccionario del Español de México*, disponible en versión electrónica en: *http://dem.colmex.mx/*.

[104] Grupo de Trabajo del Artículo 29, dictamen 4/2007 sobre el concepto de datos personales, p. 28, disponible en: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf*.

su personalidad, alguna característica física o psíquica, los rastros de su comportamiento, etcétera. La realidad contemporánea hace que prácticamente cualquier actividad que los seres humanos realicen deje una marca informativa. De manera similar, en el contexto de la UE se explica lo siguiente:

> …
> El segundo componente —"sobre"— no ha suscitado hasta ahora mucho interés, pero es crucial en la determinación del alcance sustantivo del concepto, especialmente en relación con objetos y nuevas tecnologías. El dictamen proporciona tres elementos alternativos —"contenido", "finalidad" o "resultado"— para determinar si la información versa "sobre" una persona física. Este componente abarca asimismo la información que puede tener claras repercusiones sobre la manera en que se trata o se valora a una persona...[105]

Siguiendo la lógica europea, la información será concerniente respecto al contenido si se refiere a esa persona; respecto a su finalidad si influye en la situación o comportamiento de ésta, y respecto a su resultado si el uso repercute en los derechos o intereses de ésta.[106]

La persona física debe entenderse como cualquier ser humano, bajo la regla establecida por el Código Civil Federal en su artículo 22, a saber: "La capacidad jurídica de las personas físicas se adquiere por el nacimiento y se pierde por la muerte; pero desde el momento en que un individuo es concebido, entra bajo la protección de la ley y se le tiene por nacido para los efectos declarados en el presente Código" (artículo 22, CCF). En este mismo sentido se pronuncia el dictamen en comentario, al señalar "que el cuarto componente «persona física» se centra en el requisito de que los «datos personales» se refieran a «seres vivos»".[107]

Las características de "identificada o identificable" hacen referencia a la capacidad para determinar a la persona física de entre un conjunto de sujetos. Este aspecto presupone la existencia de una persona física a la cual pueda señalarse dentro de un universo de personas a través del

[105] *Idem*.
[106] *Ibidem*, pp. 12 y 13.
[107] *Ibidem*, p. 28.

cruce de la información del individuo y del conjunto. En este sentido, la fecha de nacimiento en una credencial es de un sujeto identificado (aquel cuyo nombre y fotografía aparece en el documento), mientras que el color de cabello y la estatura de un sujeto pueden hacerlo identificable en un conjunto. Señala el texto europeo en análisis:

> …
> El tercer componente —"identificada o identificable"— se centra en las condiciones que deben darse para poder considerar a una persona como "identificable", y especialmente en "los medios que puedan ser razonablemente utilizados" por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona. El contexto y las circunstancias particulares de cada caso concreto tienen un papel importante en este análisis…[108]

Señala el RLFPDPPP que una persona identificable es toda persona cuya identidad pueda ser determinada directa o indirectamente mediante cualquier información. En sentido contrario, rechaza la posibilidad de hacerla identificable si existen medios o plazos desproporcionados para hacer dicha asociación entre la información y la identidad del sujeto (artículo 2o., fracción VIII, RLFPDPPP).

Así las cosas, los cuatro elementos: la información, la persona física, la relación establecida "respecto" —como se señala en la norma mexicana— o "sobre"—en los términos europeos— y la calidad de identificable o identificada, deben confluir para poder establecer que un determinado dato sea clasificado como dato personal.

---

c. Los datos sensibles

Otro de los conceptos necesarios para entender la protección de datos en cualquier ámbito es el de datos sensibles. Nuestra legislación los define como:

[108] *Idem*.

...

> Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual (artículo 3o., fracción VI, LFPDPPP).

Este concepto debe ligarse con la naturaleza del derecho a la protección de datos personales como un derecho fundamental. Así las cosas, dos de los principios de los derechos humanos establecidos en la CPEUM son los de indivisibilidad e interdependencia, que imbrican a los derechos entre sí en un complejo sistema. Sobre esto, se ha señalado que "son interdependientes en tanto establecen relaciones recíprocas entre ellos, y son indivisibles en la medida en que no deben tomarse como elementos aislados o separados, sino como un conjunto".[109]

Así las cosas, los datos personales sensibles son aquellos que pueden poner en riesgo la protección del derecho a la no discriminación de los titulares —y otros derechos más— por ser revelados en contextos sociales complejos. Pensemos, por ejemplo, en el caso particular de la ludopatía como un padecimiento del titular de los datos, que puede ser rastreado del patrón de comportamiento dentro de las salas de sorteos de números o símbolos y centros de apuestas remotas y cuya publicidad podría causarle un trato distinto en, por ejemplo, una solicitud de crédito.

C. *Sujetos*

El segundo componente de la relación jurídica es el ámbito de aplicación subjetiva, es decir, los sujetos involucrados. La norma señala tres componentes indispensables en la fórmula de la protección de los datos personales: el sujeto titular, el responsable y el encargado. De éstos, quizá el más sencillo de delimitar es el primero enlistado.

[109] Vázquez, Luis Daniel y Serrano, Sandra, "Los principios de universalidad, interdependencia, indivisibilidad y progresividad. Apuntes para su aplicación práctica", en Salazar, Pedro y Carbonell, Miguel (coords.), *La reforma constitucional de derechos humanos: un nuevo paradigma*, México, UNAM, Instituto de Investigaciones Jurídicas, 2011, p. 152.

Son titulares de los datos personales las personas físicas, es decir, cualquier persona que, como de antemano señalamos, se encuentra descrita en el artículo 22 del CCF. En este sentido, todas las personas físicas tienen el derecho a que su información sea tratada con diligencia bajo los principios rectores y, además, a ejercer los derechos respecto a esa información.

El segundo elemento subjetivo es el responsable. Éste es definido por la ley como aquella persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. Sin entrar en mayores detalles, el responsable es el sujeto obligado que lleva la carga en la relación jurídica que se desprende del tratamiento de los datos. En el caso que nos ocupa, son responsables los operadores y permisionarios respecto a los datos de sus clientes, sus trabajadores y demás personas físicas con las que tengan algún tipo de relación, con excepción de sus proveedores y prestadores de servicios profesionales.[110]

El encargado es una figura contingente en la relación jurídica que comentamos. Éste es definido como aquella persona física o moral distinta al responsable. Lo importante que omite el texto legal es al encargado que lleva a cabo el tratamiento de los datos personales a nombre y en representación del responsable. Es decir, es un sujeto diverso al responsable que lleva a cabo la recolección, almacenamiento o cualquier otro uso de los datos sin que exista una relación laboral en el caso de las personas físicas, o de agregación corporativa en el caso de las personas morales. Ejemplos de esta figura pueden ser las empresas de telemercadeo contratadas por los permisionarios y operadores, los prestadores de servicios de videovigilancia, de representación jurídica, etcétera (artículo 3o., fracción XVII, LFPFPPP).

En síntesis, el titular es aquel sujeto del que se trata la información; el responsable es aquella persona jurídica que lleva a cabo el tratamiento, y el encargado es aquel que, por así considerarlo necesario el responsable, lleva a cabo el tratamiento en su nombre.

---

[110] Sobre este punto es relevante asociar la excepción de aplicación del RLFPDPPP a los comerciantes y profesionistas, así como respecto a la información de contacto de los trabajadores, que se desprende de su actividad laboral.

D. *El tratamiento de datos personales*

El tratamiento de la información personal es el centro de la relación jurídica que analizamos. Conforme a lo señalado por la normatividad legal y reglamentaria, lo definimos como toda aquella actividad que se realice —activa o pasivamente— sobre la información del titular. La norma señala que la obtención, el uso, la divulgación y el almacenamiento son especies del tratamiento. Ahora bien, el uso de datos personales conlleva el acceso, el manejo, el aprovechamiento, la transferencia o disposición de los mismos.

Lo anterior implica que —pensemos en un cliente nuevo de un establecimiento— desde el momento en el que se genera un usuario, se le solicitan sus datos de identificación, el almacenamiento físico y electrónico, el registro de video en las cámaras de seguridad, su historial de juego en el caso de las máquinas electrónicas, la creación de datos estadísticos, el envío de correos electrónicos publicitarios, etcétera. Todos ellos son tipos de tratamiento protegidos por la norma.

E. *Los principios rectores*

Como señalamos anteriormente, el derecho a la protección de datos personales conlleva dos grandes elementos: los principios rectores del tratamiento y los derechos ARCO. Los primeros son las reglas por las que debe regirse cualquier actividad que se lleve a cabo con la información de las personas físicas. Son la base mínima de protección. De éstos se desprenden obligaciones particulares que recaen en los responsables, que redundan en orientaciones de comportamiento durante todos los tratamientos de datos que se lleven a cabo mientras persiste un vínculo entre responsable y titular.

Si bien se encuentran desarrollados en la LFPDPPP, son listados pedagógicamente en el Reglamento correspondiente de la siguiente manera.

De acuerdo con lo previsto en el artículo 6o. de la Ley, los responsables deben cumplir con los siguientes principios rectores de la protección de datos personales:

— Licitud.
— Consentimiento.
— Información.
— Calidad.
— Finalidad.
— Lealtad.
— Proporcionalidad.
— Responsabilidad.

Asimismo, el responsable deberá observar los deberes de seguridad y confidencialidad a que se refieren los artículos 19 y 21 de la Ley (artículo 9o., RLFPDPPP).

Tenemos entonces un catálogo de ocho principios rectores que son de aplicación transversal durante todo el uso que se le dé a la información personal. Ahora bien, el artículo arriba citado enuncia dos deberes más: seguridad y confidencialidad. Éstos se relacionan íntimamente con los principios listados y serán analizados posteriormente. Para el estudio de estos principios proponemos describirlos sucintamente para tener el entramado de conceptos que nos permitan listar y entender el vínculo con las obligaciones señaladas en la LFPDPPP y su Reglamento.

a. Licitud

El principio de licitud es quizá el más amplio de todos. Entendido de manera laxa, constriñe al responsable a actuar siguiendo los principios rectores y dando cabal garantía al ejercicio de los derechos ARCO. Ahora bien, el principio de licitud no queda reducido a esto, sino que existen obligaciones expresas para cumplir con él; por ejemplo, se enuncia en el RLFPDPPP que "el principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional".[111] La legislación mexi-

[111] Artículo 10, RLFPDPPP.

cana tiene algunas normas que se relacionan con la protección de datos personales; ejemplos de ella son los delitos de revelación de secretos y el acceso ilícito a sistemas y equipos de informática contemplados en el Código Penal Federal.[112]

Por lo que hace a la normatividad internacional, son relevantes como normas orientadoras la Resolución de Madrid[113] y las Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales.[114] Si bien no podemos asumir la obligatoriedad de éstas, al no ser propiamente tratados internacionales que formen parte del aparato normativo mexicano conforme al artículo 136 constitucional, son normativas orientadoras para gran parte de los socios comerciales mexicanos. La primera normativa es importante para el contexto global, pero con mayor énfasis en el área europea, por el modelo de privacidad establecido en éste; mientras que el segundo es de mayor relevancia para los miembros de la OCDE. Un punto particularmente relevante es el tema del juego en línea, en el que algunos socios comerciales del extranjero, como el caso de la UE, están reforzando la protección de la información que se transmite en la red de sus ciudadanos.

Las principales obligaciones relativas a este principio son:

— Cumplir de manera cuidadosa con los principios rectores.
— Recabar y tratar los datos personales conforme a la normatividad nacional e internacional.
— Tomar medidas jurídicas y administrativas para que los compromisos del tratamiento sean desarrollados por los responsables, trabajadores y encargados.

Para mayor detalle véase el anexo “Principio de licitud”.

[112] CPF, título noveno.

[113] Estándares internacionales para la protección de la privacidad, en relación con el tratamiento de datos de carácter personal, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid, España, disponible en: *http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_conferencias_estrasburgo_res_ma drid_2013.pdf.*

[114] Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales, disponible en: *http://www.oecd.org/sti/ieconomy/15590267.pdf.*

b. Consentimiento

Por regla general, el consentimiento es el punto inicial de toda relación de tratamiento de datos personales. Mediante la manifestación del consentimiento, sea cual sea su modalidad, es que el titular permite al responsable que lleve a cabo cualquier actividad con su información. Existen, en contraste, excepciones al tratamiento originado en la obtención del consentimiento, establecidas en el artículo 10 de la LFPDPPP de la siguiente manera:

— Esté previsto en una ley.
— Los datos figuren en fuentes de acceso público.
— Los datos personales se sometan a un procedimiento previo de disociación.
— Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
— Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.
— Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente.
— Se dicte resolución de autoridad competente (artículo 10, LFPDPPP).

El consentimiento debe ir ligado a datos personales concretos y, de la misma manera, a finalidades precisas. Vale la pena mencionar que los datos recabados y tratados, así como la finalidad, deberán quedar plasmados en el aviso de privacidad, del que se hablará más adelante.

Ahora bien, es importante resaltar respecto a las excepciones, que únicamente permiten al responsable dar tratamiento a los datos personales; sin embargo, este hecho no implica la excepción del cumplimiento de los demás principios, obligaciones ni de la garantía de ejercicio de los derechos ARCO.

Desde la perspectiva contraria, se exigen especies agravadas en la obtención del consentimiento. Por una parte, se requiere el consentimiento expreso cuando:

— Lo exija una ley o reglamento.
— Se trate de datos financieros o patrimoniales.
— Se trate de datos sensibles.
— Lo solicite el responsable para acreditar el mismo, o
— Lo acuerden así el titular y el responsable (artículo 15, LFPDPPP).

Desde el punto de vista de nuestro estudio, los permisionarios y operadores de salas de sorteos de números o símbolos y centros de apuestas remotas deben obtener el consentimiento expreso de los titulares en los supuestos que requieran datos financieros y patrimoniales. Como señalamos con antelación, este caso se presenta frecuentemente en los juegos con apuestas para cumplir con las obligaciones legales en materia de fiscalización hacendaria, prevención de lavado de dinero, etcétera.

Las obligaciones relacionadas con este principio son:

— Recabar de manera efectiva el consentimiento para cualquier tratamiento de datos personales.
— Atender las modalidades del consentimiento "expreso" y "expreso por escrito".
— Facilitar la revocación del consentimiento.

Para mayor detalle véase el anexo "Principio de consentimiento".

c. Información

El principio de información se adiciona al de consentimiento como uno de los requisitos previos a la relación de tratamiento de datos personales.

> Este principio se materializa principalmente en el denominado "aviso de privacidad", documento mediante el cual los responsables delimitan *ex ante* los datos personales que recabarán de los titulares, las características principales del tratamiento, las finalidades para las cuales serán tratados, entre otros detalles importantes para la relación de tratamiento de información personal.

Como obligaciones relativas al principio de información, resaltan las siguientes:

— Generar un aviso de privacidad que cumpla con los requisitos legales, reglamentarios y los criterios adicionales emitidos por el órgano garante.
— Dar a conocer el aviso de privacidad en los medios y modalidades establecidas en la norma.

Para mayor detalle véase el anexo "Principio de información".

d. Calidad

Respecto al principio de calidad, el RLFPDPPP señala lo siguiente:

> "Se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados" (artículo 36, RLPPDPPP).

Esto implica un compromiso del responsable para mantener altos estándares en la corrección de los datos personales que trata. Lo anterior tiene como propósito evitar que un error o deficiencias en el tratamiento u obtención de los datos personales tenga efectos nocivos en los titulares.

Para ahondar en las obligaciones de este principio véase el anexo "Principio de calidad".

e. Finalidad

El principio de finalidad constituye otro de los puntos torales de la protección de los datos personales. Éste se concentra en el destino que llevarán los datos personales utilizados por el responsable.

> Una de las primeras características que se deben cumplir para salvaguardar este principio es que las finalidades se encuentren definidas en el momento en el que los datos son obtenidos, y que el tratamiento se centre en la finalidad acordada entre responsable y titular. Así las cosas, es contrario a este principio recabar datos para un propósito y darles un uso distinto.

El momento oportuno para comunicar la finalidad al titular, y que éste pueda —en los casos aplicables— consentir su uso, es generalmente el aviso de privacidad antes mencionado.

Las cargas jurídicas que representa este principio son desarrolladas en el anexo "Principio de finalidad".

f. Lealtad

En complemento a los principios de consentimiento, información y finalidad, el principio de lealtad cierra un cuadrante de defensa para los titulares.

> La lealtad se refiere al compromiso del responsable para con el titular de mantener los acuerdos que se desprenden de la oferta establecida en el aviso de privacidad, señalando cuáles datos se recaban y para qué serán utilizados.

Así, si se recaban y tratan datos de manera engañosa, dolosa o negligente, el responsable se encuentra en falta respecto a este principio.

Se da cuenta de las obligaciones correspondientes a este principio en el anexo "Principio de lealtad".

g. Proporcionalidad

Otra de las máximas que se incluye en el catálogo de principios es la proporcionalidad. Ésta debe entenderse como el equilibrio necesario que se debe guardar entre los datos personales que se recaban, su grado de sensibilidad y la finalidad para la que son tratados. Así las cosas, cuando un cierto tratamiento exige que sean usados determinados datos y son éstos los únicos que se recaban y tratan, podemos decir que es un tratamiento proporcional. En sentido contrario, si se recaban datos innecesarios se dirá que el tratamiento es desproporcionado o excesivo. Así, la proporcionalidad consiste en la facultad restringida de tratar únicamente los datos personales que sean necesarios, adecuados y relevantes en relación con las finalidades preestablecidas con antelación al consentimiento.

Sobre este punto opera el criterio de minimización, que se entiende como el deber del responsable para que los datos personales utilizados en sus procesos sean los mínimos necesarios para dar cumplimiento a la finalidad establecida (artículos 45 y 46, RLFPDPPP).

Para mayor detalle se recomienda revisar el anexo "Principio de proporcionalidad".

h. Responsabilidad

El último de los principios rectores en la relación de protección de datos personales es el principio de responsabilidad. Éste debe ser entendido como la carga que tiene el responsable sobre el cumplimiento de los demás principios y obligaciones respecto a los datos personales que recabe, almacene o con los cuales lleve algún tratamiento. Las obligaciones que se desprenden de este principio se mantienen en el ámbito del responsable, aun y cuando los datos hubieran sido transmitidos a un encargado incluso fuera de la jurisdicción territorial mexicana.

Algunos de los medios por los cuales el responsable puede dar cumplimiento a este principio de manera aún más rígida a la impuesta por la normatividad mexicana es su inclusión voluntaria a esquemas de cumplimiento de estándares, mejores prácticas, políticas corporativas, certificaciones nacionales o internacionales y esquemas de autorregulación (artículos 45 y 46, RLFPDPPP).

El establecimiento de medidas de seguridad es importante para el debido cumplimiento, así como la identificación de potenciales vulneraciones a estas medidas.

El riesgo de vulneración de las medidas de seguridad de los datos personales deberá minimizarse hasta los niveles más óptimos. Si bien no existen medidas de seguridad infalibles, la prevención es de vital importancia.

Bajo el espectro de este principio encontramos las obligaciones desarrolladas en el anexo "Principio de responsabilidad".

F. *Derechos ARCO y cargas procedimentales*

Como adelantamos en la introducción a este apartado, la protección de datos personales es un tema complejo. Hasta este momento se han abordado los principios rectores del tratamiento de la información personal y las obligaciones que les corresponden, pero aún queda por desarrollar una parte toral de este derecho fundamental. Nos referimos a los derechos ARCO, siglas que sintetizan los derechos de acceso, rectificación, cancelación y oposición.

Los derechos ARCO conforman lo que algunos especialistas identifican con el "derecho a la autodeterminación informativa", entendido como "el control que [se] ofrece a las personas sobre el uso por terceros de información sobre ellas

mismas",[115] es decir, el control que existe de las personas físicas sobre sus datos personales.

A nivel constitucional, estos derechos quedaron consagrados, desde 2009, íntegramente en el artículo 16, segundo párrafo. Su desarrollo normativo se encuentra en la LFPDPPP y en su Reglamento. Ahora daremos cuenta sumariamente de su contenido esencial y se dará paso a la descripción de las actividades a las que se obliga a los titulares para el ejercicio de estos derechos.

El derecho de acceso a los datos personales consiste en la facultad que tiene todo individuo a solicitar, y a que le sean comunicados, los datos personales que obren en bases de datos o cualquier sistema de almacenamiento por parte de un sujeto obligado, así como los detalles respecto del tratamiento de estos datos. El ejercicio de este derecho se ve cumplimentado al momento de poner a disposición del titular la información solicitada.

El derecho de rectificación se relaciona íntimamente con el principio de calidad antes mencionado. Si existe una obligación de mantener los datos actualizados y correctos por parte del responsable, es un derecho de los titulares solicitar que se hagan los ajustes necesarios a los datos que sean inexactos o estén desactualizados.

Los siguientes derechos se derivan del principio de finalidad. Ante el cumplimiento de la finalidad para la cual los datos fueron recabados, opera el derecho de cancelación. En últimas consecuencias, este derecho consiste en la supresión de la información que, al haber cumplido la finalidad establecida, es innecesario que continúe en poder del responsable. Para llegar al punto de su supresión, según la LFPDPPP y su Reglamento, se debe pasar por un periodo de bloqueo, que consiste en el resguardo de la información personal por un tiempo, que dependerá de los periodos de caducidad y prescripción de las obligaciones inherentes a las relaciones jurídicas que hubieran dado lugar al tratamiento.

[115] Murillo de la Cueva, Pablo Lucas, "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en Murillo de la Cueva, Pablo Lucas y Pinar Mañas, José Luis, *El derecho a la autodeterminación informativa*, México, Fontamara, 2011, p. 11.

Por último, tenemos el derecho a oponerse a un determinado tratamiento. Este derecho implica el cese en el uso de los datos personales por parte del responsable, ya sea para el tratamiento completo, o bien para una finalidad particular. En el primero de los supuestos se requiere que exista una causa que pueda originar un perjuicio al titular. El segundo, en cambio, opera para aquellas finalidades de las que no depende alguna obligación jurídica. El caso paradigmático de la segunda hipótesis es la oposición para el telemercadeo, las listas de exclusión, etcétera.

Ahora bien, para el ejercicio de estos derechos por parte de los titulares, el legislador ha previsto una serie de medidas a cargo del responsable. En síntesis, se trata del establecimiento de un procedimiento de ejercicio y las cargas inherentes a éste, como la designación de una persona o un departamento para la atención de las solicitudes.

Existe un quinto derecho que debe tratarse de la misma manera que los derechos ARCO, a saber: la revocación del consentimiento, establecido en el artículo 8o. de la LFPDPPP.

Como se hizo en los puntos anteriores, se presentan en el anexo "Derechos ARCO" las obligaciones inherentes al ejercicio de estos derechos y algunas cargas procesales dependientes de este mecanismo.

2. *Derecho comparado*

Para llevar a cabo un análisis comparado de los regímenes de protección de datos personales es necesario tomar en cuenta el punto de partida desde el cual se realiza el estudio en cuestión. Los resultados del escrutinio comparativo entre diversos sistemas normativos dependerán del marco inicial del que se lleve a cabo la investigación. Así las cosas, para la elaboración de un estudio que tenga como objetivo analizar individualmente cada sistema y comparar los resultados de cada análisis entre sí, o bien tomar un modelo como punto de partida y resaltar las diferencias de los modelos analizados con el sistema referente.

Para el presente apartado hemos optado por el segundo modelo, al considerar que el objetivo del estudio en conjunto se cumple a cabalidad poniendo énfasis en los contrastes. Para hacer esto, se ha decidido tomar como modelo referente al sistema de protección de datos personales en

posesión de los particulares en el caso mexicano. Lo anterior tiene como fundamento el avance legislativo y reglamentario de carácter reciente en nuestro país, cuya normatividad más importante supera apenas un lustro y se encuentra en algunos temas mucho más avanzada en relación con los otros sistemas a estudio. Además, el modelo analizado en los puntos anteriores recoge casi en su totalidad los elementos torales del modelo de protección de datos personales que se ha convertido en piedra de toque para las autoridades garantes en la Resolución de Madrid.[116]

En este sentido, se analizarán los modelos europeo y norteamericano en los casos particulares de España, Inglaterra y Estados Unidos de América, con especial énfasis en los estados de Nevada, Nueva York y Nueva Jersey, a través del lente puesto por el modelo mexicano analizado con anterioridad.

A. *El modelo europeo*

El derecho a la protección de datos personales es una creación europea, en específico alemana. Contrario a la *privacy* norteamericana, como veremos más adelante, es un derecho concentrado al resguardo de un aspecto concreto de la persona: su información. Desde su nacimiento en la República Federal Alemana, mediante la sentencia del 15 de diciembre de 1983 relativa a la Ley del Censo, el derecho a la autodeterminación informativa se constituyó como un derecho fundamental.

La visión de la protección de la información personal desde la perspectiva iusfundamental, aunada al avance tecnológico en las comunicaciones y tecnologías de la información, generó que el derecho fuera adoptado progresivamente en las nuevas Constituciones europeas de la segunda mitad del siglo XX,[117] para luego ser incorporado en los instrumentos que darían sustento a la UE.

Uno de los principales resultados de este proceso es la Directiva 95/46/CE, cuyo contenido afecta directamente las disposiciones de dos

[116] Declaración de Madrid, *op. cit.*, nota 14.

[117] El ejemplo español es detallado por Piñar Mañas en Murillo de la Cueva, Pablo Lucas, "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", *op. cit.*

de nuestros modelos normativos de análisis: el español y el del Reino Unido.

Las principales características del esquema regulatorio europeo son las siguientes: se reconoce el derecho a la protección de datos personales como un derecho fundamental; existe una normatividad general para los sectores público y privado que desarrolla profundamente las regulaciones del derecho a la protección de datos personales; se cuenta con un conjunto de principios rectores y con un órgano especializado para dar seguimiento a la implementación del cumplimiento de los principios rectores y para garantizar mediante procedimientos administrativos sencillos los derechos del titular.

En materia de principios rectores, se establecen el de licitud, lealtad, finalidad, calidad, proporcionalidad y legitimación, todos consignados en el artículo 6o. de la mencionada Directiva.

Este marco regulatorio, al igual que el mexicano, no distingue las actividades o sectores económicos para los que se lleva a cabo el tratamiento de los datos. La figura del responsable es homogénea a las definiciones mexicanas y la regulación es aplicable a la industria del juego con apuestas.

Sobre este punto, es destacable mencionar que la Comisión Europea ha explicitado la aplicación de la Directiva 95/46/CE a la industria del juego con apuestas. Ejemplo de esto es el *Libro verde sobre el juego en línea en el mercado interior*, de la siguiente manera: "En relación con la legislación derivada europea, y si bien los servicios de juego no están regulados por ninguna normativa sectorial específica a nivel de la UE, quedan, no obstante, sujetos a lo dispuesto en [la] Directiva sobre Protección de Datos".[118]

Una de las principales diferencias entre el modelo mexicano y el europeo es el principio de legitimación en relación con el principio de consentimiento mexicano. Mientras un tratamiento legítimo se circunscribe en el caso mexicano al externamiento fehaciente y libre del consentimiento para que la información personal sea tratada, y a éste se le incluyen excepciones para su obtención, el modelo europeo reconoce cuatro supuestos en los que se considera legítimo el tratamiento:

[118] Comisión Europea¸ *Libro verde sobre el juego en línea en el mercado interior*, publicado el 24 de marzo de 2011 y disponible en línea en: *http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52011DC0128&from=EN.*

— El consentimiento.
— La necesidad de tratamiento para el cumplimiento de relaciones contractuales.
— El cumplimiento de obligaciones jurídicas.
— El cumplimiento de una misión de interés público (artículo 7o., Directiva 95/46/CE).

Esta distinción es importante. Si bien algunas de estas causas de legitimación coinciden con nuestras excepciones de obtención del consentimiento, el punto de partida para el tratamiento deja claro en el modelo europeo que el tratamiento debe ajustarse a la normatividad aun y cuando no sea requerido el consentimiento, ya que se realiza el tratamiento con fundamento en una causa legítima. En contraste, el modelo mexicano causa confusión entre los responsables, ya que al excusar del único fundamento legítimo, parece que el tratamiento exceptuado lo exime del resto de sus responsabilidades.

Aunado a lo anterior, la existencia de manifestación directa del consentimiento genera una carga fuerte para el responsable, que se encuentra impedido en muchos supuestos en la realización de las actividades que relacionen datos personales, entorpeciendo sus labores naturales.

Uno de los principios considerados en el modelo mexicano y que no es desarrollado como tal en el modelo europeo es el de información. En nuestro modelo se hace efectivo a través del aviso de privacidad —con todas las obligaciones ya revisadas al respecto—, mientras que en el modelo europeo se reduce a incluir la siguiente información:

— La información del responsable y, de ser el caso, de su representante.
— Los datos personales recabados y las finalidades del tratamiento.
— Los destinatarios de los datos y sus categorías; la existencia de los derechos de acceso y rectificación correspondientes, etcétera (artículo 10, Directiva 95/46/CE).

El principio de responsabilidad tampoco se considera en el modelo europeo como un principio rector; en cambio, se le impone al responsable una serie de obligaciones en materia de seguridad de la información.

Vale la pena señalar que estas últimas coinciden con las que hemos analizado en el modelo mexicano. Dentro de éstas destacan:

— El establecimiento de medidas técnicas y de organización para la prevención de su destrucción o pérdida accidental o ilícita; difusión, acceso y alteración no autorizados; o cualquier tratamiento indebido.
— La designación de encargados calificados en la materia para el tratamiento de los datos.
— La formalización contractual de las tercerizaciones de tratamientos por encargo.
— La documentación de las medidas de seguridad adoptadas (artículo 17, Directiva 95/46/CE).

Otra de las distinciones con el modelo europeo es la notificación a la autoridad de control.[119] Esta obligación se cumple al notificar al órgano garante de cualquier sistema de tratamiento de datos personales; en consecuencia, los órganos garantes deben contar con una base de datos que contenga todos y cada uno de los sistemas de tratamiento automatizados de datos personales. Al imaginar el volumen que esta carga conlleva, no es difícil entender las razones para su supresión en la Directiva (artículo 26, Directiva 95/46/CE).

En materia de derechos, se encuentran reconocidos los cuatro derechos ARCO. El derecho de acceso incluye tanto la posibilidad de acceder a la propia información personal como a los detalles del tratamiento y los tratamientos automatizados. Por su parte, la corrección y cancelación se encuentran sujetas a que los tratamientos no se ajusten a la Directiva, sean inexactos o incompletos. Por último, el derecho de oposición se prevé para finalidades determinadas.

Como vemos, el modelo de protección de la información personal es similar al mexicano. Salvo las distinciones entre los principios de legitimación y responsabilidad, y las obligaciones relativas a la notificación de la creación de sistemas de tratamiento automatizados, son esquemas regulatorios altamente compatibles.

[119] Aunque esta característica ha sido eliminada en las recientes actualizaciones a la Directiva en análisis, siguen vigentes para los Estados a analizar, por lo que es menester hacer mención de ella.

Lo anterior representa una ventaja competitiva para los operadores y permisionarios, quienes fácilmente pueden acceder al público europeo preocupado por la seguridad y protección de sus datos, sea en forma presencial en las salas de sorteos de números o símbolos o en centros de apuestas remotas operados en nuestro país, o en corridas de apuestas vía remota.

Es menester señalar que el bloque europeo se encuentra en proceso de actualización. Ante las reformas iniciadas en 2012 y finalmente acordadas y publicadas el 6 de mayo de 2016, los países integrantes del bloque europeo deberán actualizar su legislación interna a las nuevas normas comunitarias actualizadas a más tardar el 6 de mayo de 2018. Lo anterior debe sumarse al proceso de salida del Reino Unido de la misma comunidad, lo que potencialmente afectará tanto las normas de Inglaterra, Escocia e Irlanda del Norte, así como, sustancialmente, el alcance y proyección del modelo europeo.

Algunas de las modificaciones al marco regulatorio son:

— Eliminación de la obligación de notificación.
— Aumento en las obligaciones de seguridad.
— Previsión de herramientas sencillas para el acceso a los datos personales.
— Derecho al olvido.
— Notificación de ataque *hacker*.

Todas previstas por la legislación mexicana.

Una vez planteado el escenario europeo, la descripción de los esquemas de protección de datos tanto español como británico serán muy sucintos. Se hace énfasis en las diferencias sustantivas que no se corresponden con el modelo mexicano. El esquema que se usará empleará un recuento del entramado normativo institucional para cada país y algunos detalles importantes.

a. España

En España, el derecho a la protección de datos personales no se encuentra establecido explícitamente en el ordenamiento constitucional; sin embargo, la protección establece la limitación de la informática para

garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (artículo 18.4 de la Constitución Española de 1978).

Bajo esta tesitura, en 1992 se promulgó la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), que tuvo el mandato de desarrollar el contenido del artículo constitucional. Esta disposición normativa fue sustituida en 1999 por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), debido a la entrada en vigor de la Directiva 95/46/CE, desarrollada con antelación.

La aplicación de la LOPD está destinada a los datos de carácter personal registrados en soporte físico y a todas las modalidades de uso de los datos para el sector público y privado. En contraste, la normatividad mexicana está especializada en el sector privado y se encuentra en un proceso de reforma general en el sector público desde 2014. A la LOPD se le suma el Reglamento respectivo de 2007 (RDLOPD). Para dar cumplimiento a estas disposiciones normativas se creó la Agencia Española de Protección de Datos (AEPD). Para el caso de las Autonomías se previó la creación de órganos garantes locales, cuya tarea es la aplicación de las normas en las esferas públicas bajo su jurisdicción; en consecuencia, podemos afirmar que para los operadores y permisionarios de casinos y figuras similares la jurisdicción queda encomendada a la AEPD.

En relación con los principios rectores, el esquema regulatorio español recoge el principio de consentimiento (artículo 6o., LOPD). Es destacable que el esquema de consentimiento español pasó integralmente al modelo mexicano y se separa del principio de legitimación europeo. El principio de calidad español incluye medidas significativamente similares a nuestros principios de proporcionalidad y finalidad (artículo 4o., LOPD).

El principio de información obliga al responsable a informar, en el momento que se obtienen los datos:

— La existencia de ficheros (bases de datos) de información personal.
— La obligatoriedad o no de la disposición de los datos (preguntas de respuesta obligatoria para la obtención de un determinado servicio).

— Las consecuencias de la obtención de los datos o la negativa a proporcionarlos.
— Identidad y domicilio del responsable.
— Los derechos ARCO (artículo 5o., LOPD).

La LOPD enumera bajo la figura de "seguridad de los datos" lo que en el modelo mexicano se estableció como principio de responsabilidad. La seguridad de los datos se centra en la creación de medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado (artículo 9o., LOPD).

Se prevén medidas que el legislador español ha entendido como parte del principio de lealtad. En este sentido, el deber de secreto, las protecciones de la comunicación de los datos y el control sobre el acceso a los datos por parte de terceros se identifican con las obligaciones establecidas en este principio (artículos 10, 11 y 12, LOPD).

Por lo que hace a los derechos de los titulares, el modelo español recoge los derechos de acceso, rectificación, cancelación y oposición, aunados al derecho de consulta del Registro General de Protección de Datos. Por lo que hace al derecho de acceso, se prevé notificar sobre la información relativa a los datos del titular, el origen de los datos, así como a las comunicaciones de los mismos. El acceso está garantizado de manera gratuita y se prevén múltiples medios para su ejercicio. Los derechos de rectificación y cancelación, al igual que en el modelo europeo, se vinculan a los tratamientos que se distancien de la LOPD, sean incorrectos o incompletos. El modelo español prevé el periodo de bloqueo mencionado para el caso español y las obligaciones para los encargados arriba descritas. El derecho de oposición se encuentra relacionado con los fines de prospección y publicitarios exclusivamente. En este caso, el modelo mexicano abarca una mayor cantidad de supuestos (artículos 15, 16, 17 y 30, LOPD).

Una de las principales diferencias entre los modelos europeo y mexicano se presenta también para el caso español. Como hemos dicho, los responsables tienen la obligación de notificar y registrar los ficheros de datos personales bajo su custodia. En el caso español, dicho registro se denomina Registro General de Protección de Datos y queda bajo la supervisión de la AEPD. En contrapartida, los titulares tienen derecho a conocer

dicho registro. Para el caso mexicano esta prerrogativa no es aplicable (artículo 14, LOPD).

Como en el caso mexicano, la LOPD prevé procedimientos y cargas a los responsables para dar respuesta a las solicitudes de ejercicio de los derechos ARCO. Una característica destacable es el derecho a ser indemnizado por el daño o lesión en bienes o derechos del titular por los incumplimientos que pudiera cometer el responsable (artículos 18 y 19, LOPD).

Por último, no es óbice señalar que el modelo español también prevé infracciones, procedimientos administrativos y sanciones para salvaguardar el cumplimiento de las disposiciones en la materia. Las multas para el caso español ascienden a los 600 mil euros, esto es, superiores a doce millones de pesos.

b. Reino Unido

Al igual que en el caso español, el Reino Unido no prevé disposiciones constitucionales que garanticen específicamente el derecho a la protección de datos personales. Para las comunidades de Gales, Inglaterra e Irlanda del Norte, el derecho a la protección de datos personales tiene su origen en las normas de la comunidad europea. El modelo normativo vigente se encuentra desarrollado en la *Data Protection Act* (DPA) de 1998. Como órgano garante se estableció al *Information Commissioner* (ICO), que tiene a su cargo también, como ocurre con el INAI en el caso mexicano, la vigilancia y garantía del acceso a la información pública.

Ahora bien, por lo que hace al modelo regulatorio hemos adelantado que el modelo británico se ciñe a lo determinado por la Directiva 95/46/CE, y se concentra en el establecimiento de principios rectores, obligaciones derivadas de éstos, los derechos ARCO, procedimientos de ejercicio de derechos, procedimientos de vigilancia, un conjunto de infracciones y sanciones.

En el ámbito de los principios, se establece que la información debe ser tratada de forma justa y lícita. Este principio lo podemos identificar con el principio de licitud mexicano. Asimismo, se establece como parte del tratamiento lícito que se apegue a una finalidad legítima (parte I, catálogo 1, DPA).

Se reconocen también los principios de proporcionalidad en relación con las finalidades establecidas, la calidad de los datos, el establecimiento de finalidades determinadas y la previsión de tratamientos con atención a los derechos del titular. También se prevé el establecimiento de medidas de seguridad técnicas y administrativas para la prevención de incidentes de pérdida, destrucción o daño a los datos personales. Se identifican estas obligaciones con el principio de responsabilidad de la LFPDPPP (parte I, catálogo 1, DPA).

Aunado a lo anterior, se prevé que la información personal obtenida se encuentre destinada a finalidades limitadas, y se establecen requisitos y procedimientos para el reconocimiento de las finalidades legítimas y proporcionales al tipo de tratamiento que se quiere dar a los datos (parte I, catálogo 1, DPA).

Por su parte, se desarrolla el principio de consentimiento exclusivamente para aquellos casos en los que la obtención de los datos se da directamente del titular, o bien cuando se presentan relaciones jurídicas entre titular y responsable. A este principio se suman las excepciones para la obtención del consentimiento, cuando el tratamiento sea necesario para:

— La administración de justicia.
— El ejercicio de facultades u obligaciones establecidas en la ley.
— Las funciones de la Corona o del gobierno.
— Para el ejercicio de funciones públicas.

Al igual que los modelos español y mexicano, el caso inglés requiere el consentimiento explícito para el tratamiento de los datos personales sensibles (parte I, catálogos 2 y 3, DPA).

El modelo inglés establece como un principio el tratamiento conforme a los derechos del titular. Específicamente, se reconocen los siguientes derechos:

— El derecho de acceder a una copia de la información en resguardo.
— El derecho de oposición.
— El derecho de oponerse al tratamiento para fines publicitarios.

— El derecho a la rectificación o cancelación de datos incorrectos. El derecho a ser compensados por tratamientos inadecuados (parte II, DPA).

Al igual que el modelo español, la DPA establece el deber de informar al ICO sobre los procedimientos de datos personales que se lleven a cabo bajo la jurisdicción británica. Se señala la prohibición de tratamiento previo al registro, las características que debe tener este registro, aunado a los deberes de notificar los cambios en los detalles del procedimiento (parte III, DPA).

Finalmente, es de hacer notar que las infracciones no están determinadas en un catálogo como en los casos mexicano o español, sino que se refieren a cualquier incumplimiento de las obligaciones de la DPA. Los montos de las sanciones ascienden a las 500 mil libras. Para 2015 se impusieron 18 multas por más de 2,031,250 libras,[120] cantidad equivalente a más de 50 millones de pesos.

B. *El modelo estadounidense*

Como adelantamos en apartados anteriores, en los Estados Unidos de América existe una aproximación abismalmente distinta a las que se han presentado hasta este momento. Es correcto afirmar que no hay un esquema regulatorio integral para la protección de la información personal, sino que existe una variedad de leyes y normativas federales y estatales que protegen de una u otra manera esta información.

Como punto de partida, debemos establecer que para los norteamericanos no existe un derecho a la protección de datos personales que sea autónomo. En cambio, han desarrollado un acercamiento diferente, la denominada *privacy*. Este derecho, contrario a lo que comúnmente se piensa, no es coincidente con lo que entendemos como derecho a la vida privada o privacidad; es mucho más amplio e incluye, según Anita L. Allen, los siguientes ámbitos de protección o concepciones de *privacy*:

[120] IT Governance LTD, *Data Protection Act (DPA) and EU GDPR Penalties*, disponible en: *http://www.itgovernance.co.uk/dpa-penalties.aspx*.

— Asociativa.
— Informativa.
— Física.
— Decisional.
— Propietaria.
— Intelectual.

Sin entrar en detalles innecesarios, bajo estos ámbitos de protección se identifican desde la protección del domicilio y las comunicaciones, la protección de la información personal, hasta el ejercicio del derecho al aborto. El ámbito que nos interesa es la denominada *informational privacy*, que Allen define como "el acceso limitado a la información personal o sensible, confidencial y la anonimidad". Se debe entender esta última como el acceso limitado a la información relativa a las personas y el control sobre esta información.[121] Una vez dicho lo anterior, es preciso identificar algunas características del modelo norteamericano de regulación en materia de protección de datos personales.

El entramado normativo es disgregado en dos vertientes: sectorial y federado. Por sectorial nos referimos a la existencia de normas para diversas ramas de las actividades económicas privadas y del sector público; por ejemplo, existen normas para el resguardo de la información financiera, como la *Fair Credit Reporting Act* (FCRA) y la *Fair and Accurate Credit Transactions Act* (FACTA); para el sector salud, la *Health Insurance Portability and Accountability Act;* o bien, para la protección de grupos vulnerables, la *Children's Online Privacy Protection Act* (COPPA), para el caso de los menores de edad que realicen actividades en línea.

La diversidad normativa respecto al nivel de gobierno es también importante. En este sentido, se encuentran regulaciones federales como las antes mencionadas, así como normas locales que desarrollan la protección de la información en la jurisdicción de los estados que integran la unión americana. Un caso paradigmático es el de California, que cuenta con un gran desarrollo en la materia a través de la *Online Privacy Protection Act* de 2003 (OPPA).

[121] *Cfr.* Allen, Anita L., "First Amendment Privacy and the Battle for Progressively Liberal Social Change", *Journal of Constitutional Law*, Universidad de Pensilvania, 2012, pp. 886-888.

Por lo que hace a las autoridades garantes de este derecho, la multiplicidad de normas, sectores y niveles normativos genera un entramado complejo y difícil de seguir para determinar qué autoridad es competente para dar seguimiento al cumplimiento e infracciones cometidas respecto a la información personal. El principal ente regulador es la *Federal Trade Commission* (FTC), que tiene a su cargo la vigilancia de la *Federal Trade Commission Act* de 1914, en cuya sección 5 se establece que quedan prohibidas las prácticas injustas o negligentes que afecten el comercio. Bajo este pequeño enunciado, la FTC ha podido imponer hasta 32.5 millones de dólares en multas por conductas contrarias a la privacidad de los usuarios.

El sector del juego con apuestas en los Estados Unidos de América no cuenta con regulación particular. En cambio, le son aplicables de manera indirecta las obligaciones relativas a la información financiera y para la prevención de fraudes y robo de identidad, o bien aquellas que regulan genéricamente a los comercios.

Ahora bien, como foco de atención para este trabajo se ha previsto el análisis de los estados de Nevada, Nueva Jersey y Nueva York en los Estados Unidos de América. Es preciso hacer notar que la falta de uniformidad en la regulación de sector a sector y de estado a estado complica en demasía la ubicación de obligaciones particulares para los operadores de casinos.

a. Nevada

De acuerdo con Karl Rutledge, Glenn Light y Kade Miller,[122] las principales obligaciones en materia de información personal para los casinos en el estado de Nevada son las contenidas en el capítulo 603 A de los Estatutos Revisados de Nevada concernientes a la seguridad de la información personal. De éstas destacan:

— Establecer medidas para la eliminación de registros de información personal cuando sean innecesarios.
— Establecer medidas de seguridad para proteger la información personal contra incidentes no autorizados que comprenden: el

[122] Light, Glenn *et al.*, "Casino Player Clubs & Nevada's Data Protection Requirements", *Gaming Management*, diciembre de 2013.

acceso, la obtención, destrucción, alteración o publicación de la información personal.
— Formalización vía contractual si se pretende publicar información personal.
— Adoptar medidas de seguridad altas para el caso del pago y transferencia de información derivados del uso de tarjetas bancarias.
— Notificación en caso de vulneración de las medidas de seguridad.

Como podemos observar, estas obligaciones se identifican con algunas de las revisadas para los casos europeo y mexicano. En particular, aquellas derivadas de los principios de responsabilidad y proporcionalidad establecidos en el caso mexicano.

b. Nueva Jersey

Para el caso de Nueva Jersey, encontramos leyes que pretenden proteger la información personal de los titulares; sin embargo, la única aplicable directamente a los casinos es el título 56:8-163 de los Estatutos del estado, que se refiere a la notificación de vulneraciones a las medidas de seguridad establecidas para la información personal.

c. Nueva York

Si bien el estado de Nueva York tiene una regulación bastante parecida al modelo europeo respecto a la información personal tratada por autoridades, la *Personal Privacy Protection Law* (Public Officers Law, artículo 6-A, secciones 91-99) de 1984, para el rubro de casinos y otros tipos de comercio no se encontraron datos que permitan identificar obligaciones particulares, con excepción de lo establecido en la *New York General Business Law 899 (Notification; person without valid authorization has acquired private information)*, que establece la obligación y características que debe tener la notificación de vulneraciones a las medidas de seguridad para la información personal.