La protección de datos personales en el ámbito electoral en el Estado de México

Sandra Ivette Razo de la Paz*

Resumen

En este ensayo se busca hacer una introducción genérica sobre la protección de datos personales, para, posteriormente, adentrarse en el tema desde un punto de vista no sólo técnico sino también filosófico para dimensionar, con apoyo en la doctrina lo que en torno al tema se ha desarrollado internacionalmente, el alcance que puede darse a la interpretación jurídica de la protección de datos personales, no obstante que en el Estado de México el marco normativo sea deficiente. Lo anterior se aterriza en el análisis de un recurso de apelación promovido por un partido político en contra de la negativa del IEEM de transmitirle datos personales, en donde el Tribunal Electoral del Estado de México (TEEM) determinó instruir la entrega de los datos, en violación a la garantía de autodeterminación informativa de los titulares de datos personales. Esto antes de la publicación de la ley de datos personales en el Estado de México

Palabras clave: datos personales, autodeterminación informativa, base de datos personales, dato personal sensible, datos personales disociados.

Abstract

In this essay look for to make a generic introduction about of the protection of personal data, for, subsequently, it enters in the theme since a point of view not only technique but philosophical as well. This with the fin to ponder the scope that it can give to the legal interpretation of the protection of personal data, with the support in the doctrine that round the theme has been developed internationally, nevertheless that in the State of Mexico the normative framework be deficient. The previous settle down in the analysis of recourse of appellation promoted by a

* Licenciada en Derecho por la Universidad Nacional Autónoma de México. Ha prestado sus servicios en el Instituto Federal de Acceso a la Información (IFAI) y en el Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios (Infoem). Actualmente, se encuentra adscrita a la Secretaría Ejecutiva General del Instituto Electoral del Estado de México (IEEM).

politic party against the negative of the IEEM to transmit him personal data, in where Electoral Court of the State of Mexico (TEEM) determined to instruct the handing over of the data, in violation to the guaranty of informative self-determination of the incumbents of personal data. This before the publication of the law of personal data in the State of Mexico.

Key words: personal data, informative self-determination, personal data base, sensitive personal data, personal data dissociated.

Introducción

En el primer apartado se pretende sensibilizar al lector para que analice el derecho de acceso a la información pública en materia electoral no únicamente desde las disposiciones y principios del derecho electoral, sino valorando también aquello que rige el derecho a la protección de datos personales más allá de la norma. En el segundo apartado se describen los conceptos jurídicos necesarios para comprender qué es un dato personal y en qué consiste su protección. En el tercer punto se expone por qué si el uso de datos personales se ha dado durante siglos, ha cobrado relevancia en estos años y su tratamiento implica grandes complicaciones con el avance de las nuevas tecnologías. En el cuarto punto se explica en qué consiste la protección de datos personales y se exponen los principios reconocidos internacionalmente para garantizarla. En el quinto punto se aterriza el análisis del marco normativo que rige a la protección de datos personales en el Estado de México hasta antes de la publicación de la ley respectiva. En el sexto y último punto se examina una determinación del TEEM, en donde si bien revisó los argumentos de protección de datos personales y la normatividad, determinó que la protección de datos personales no es aplicable a los partidos políticos en su calidad de integrantes del Consejo Distrital, en perjuicio del derecho a la autodeterminación informativa, en virtud de que en ese momento no existía la Ley de Protección de Datos Personales del Estado de México (LPDPEM).

La protección de datos personales en el ámbito del derecho electoral

Las autoridades electorales deben proteger los datos personales, para ello es menester que se tomen las medidas técnicas y materiales necesarias, que se vuelva práctica común entre servidores electorales y autoridades judiciales y que se

dé al tema la relevancia que verdaderamente amerita; sin embargo, debemos sembrar una semilla entre las autoridades para que al tomar determinaciones relacionadas con el uso, tratamiento y transmisión de datos personales lo hagan bajo una valoración general del derecho, pues la alta especialización que se ha logrado en el estudio de la dogmática jurídica ha provocado que olvidemos que el derecho es uno solo dividido en ramas para su estudio.

Para lograrlo, es indispensable incluso iniciar desde la filosofía del derecho, pues aunque pueden existir principios filosóficos de diferentes ramas que se contraponen, en algún momento esas ramas siempre se tocan. Es tan sencillo como pensar que un fideicomiso público pueda entenderse sin el derecho civil. De igual forma, el derecho electoral encuentra apoyo y sustento en otras ramas del derecho, como el civil, el penal o el constitucional. Por ello, pretendemos que en el derecho electoral se tomen en cuenta los principios y disposiciones rectores de la protección de datos personales, aunque, por lo menos en nuestro país, no sea una rama autónoma del derecho, ya que a la fecha es una consecuencia del derecho de acceso a la información;[1] no obstante, en el ámbito filosófico los principios rectores del derecho de acceso a la información justamente se contraponen con los de protección de datos personales y exitosamente coexisten sin grandes problemas.

En fin, nos enfocaremos a analizar cómo podemos aplicar esta aún incipiente protección a las personas y su información a la práctica del derecho electoral, pues se trata de un tema apenas en construcción, por lo que en lugares como el Estado de México, hasta antes de la publicación de la LPDPEM, se contaba tan sólo con unos cuantos artículos en una ley no especializada en datos personales;[2] no obstante, es posible armonizar los principios de uno y otro; incluso desde el reducido margen de interpretación que nos permite el derecho electoral podemos llevar a la práctica la protección de datos personales en casos específicos y recurrentes. Con lo anterior, se propone romper con los criterios actuales de interpretación de los tribunales electorales en cuanto al acceso a datos personales (aunque hay avances, éstos aún no son signi-

[1] El derecho fundamental de acceso a la información que se garantiza en México, principalmente a nivel federal, es ejemplo a nivel mundial, tanto por los avances normativos como por la implementación que se ha logrado del mismo.

[2] Al momento del análisis del caso, únicamente se contaba con la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios como necesaria limitante del derecho de acceso a la información pública y sus disposiciones en el tema de protección se limitan a tres artículos de la ley más un capítulo de seis artículos para el procedimiento de acceso y corrección de datos personales que no han sido abrogados.

ficativos) y dar como resultado una nueva cultura en el tratamiento, uso y transmisión de datos personales, pues no debemos dejar de lado que la base de datos más importante que se tiene en el país es el Padrón Electoral —además de las listas nominales— generado por el Instituto Federal Electoral (IFE), el cual contiene información relevante de los ciudadanos de este país.

Qué es un dato personal y los conceptos jurídicos relevantes en torno a su protección

Un dato personal es cualquier información referente a una persona física que nos permita identificarla o hacerla identificable; por ejemplo, el nombre o la imagen de una persona son los primeros datos para conocer de quién se trata y por ende a quién corresponde ese dato personal. Las características físicas aisladas, como talla, estatura y color de piel, no pueden revelar a su titular, pero relacionadas unas con otras en determinado grupo nos permiten hacer identificable al titular. Así como esta información, las preferencias sexuales; los antecedentes médicos; las preferencias políticas o religiosas; la pertenencia a determinados grupos deportivos, políticos o sindicales; los gustos por colores, música y pasatiempos son información que puede hacer a una persona física identificada o identificable.

Cuando nos referimos a personas físicas, se trata de individuos de la especie humana, hombres y mujeres sin ninguna limitación. Las personas morales o jurídico-colectivas, según la denominación que se les dé en las diversas disposiciones civiles vigentes, no tienen datos personales, por lo que esta información no puede ser motivo de la protección que se promueve en este artículo. El domicilio de una empresa con personalidad jurídica reconocida, su Registro Federal de Contribuyentes o su patrimonio no constituyen datos personales, así como tampoco el domicilio o el presupuesto de una institución de naturaleza pública, como los institutos electorales o los tribunales.

Ahora bien, no todos los datos personales tienen la misma jerarquía. El nombre de una persona es un dato personal utilizado esencialmente para distinguirla de los demás, pero hay datos personales cuya difusión puede generar problemas o conflictos a su titular en cuanto a su relación y convivencia con el resto de la sociedad. De tal suerte, dar a conocer si determinada persona tiene una preferencia sexual distinta a la convencional puede propiciar

discriminación en sus círculos familiar, social o laboral. Por tal motivo, los estudiosos del tema se han dado a la tarea de distinguir como datos personales sensibles a todos aquéllos que puedan causar o propiciar discriminación hacia su titular (Sánchez, 2009, p. 12).

El manejo de datos personales sensibles, como en el caso anterior, podría propiciar despidos laborales, rechazo o la negativa a brindar servicios de salud. En relación con lo dicho, existen datos personales que por las consecuencias desfavorables que pudiera generar su publicidad requieren mayor atención por parte de quienes los guardan y, sobre todo, mayor seguridad para evitar su empleo con fines distintos a los que originaron su recolección. Los datos personales utilizados por las instituciones electorales son importantes en cantidad, aunque no necesariamente sean datos sensibles, y un mal manejo puede ayudar a otras personas a cometer el delito de robo de identidad, no olvidemos que la credencial de elector tiene fotografía, domicilio, edad y hasta la huella digital.

Sabemos que toda la información de nosotros como personas físicas que nos haga identificables constituye nuestros datos personales de los que somos titulares. También sabemos que nos da derecho a decidir sobre ellos; en otras palabras, tenemos la propiedad de esa información y la facultad de decidir cuándo, cómo y dónde usarla, a quién aceptamos entregársela, para qué y por cuánto tiempo. A este derecho de decidir sobre el uso, destino y transmisión de datos personales se le conoce como autodeterminación informativa, esto es, el control sobre los propios datos personales. Esta autodeterminación informativa también genera obligaciones para las personas que reciben, usan o resguardan datos personales y consiste en usarlos únicamente bajo los términos de la autorización que otorgan los titulares (Carranza, 2001, pp. 23-25).

Para considerar la información de las personas como datos personales, es necesario que los esfuerzos para identificar a su titular no sean desmedidos; verbigracia, tenemos tres datos personales: sexo femenino, usa lentes y votó por el partido político que ganó en el último proceso electoral. Esta información en un grupo de 20 personas nos permitiría conocer al titular de los datos personales sin esfuerzos desmedidos, pues del reducido número que integra la muestra se descarta a los hombres y a las mujeres que no usan lentes, por lo que seguramente

quedará un grupo tan pequeño que identificaremos a la mujer de quien se revela su preferencia electoral sin esfuerzos desmedidos, esto sin dejar de lado que el secreto del voto es un derecho constitucional. Sin embargo, si con esos datos tratamos de identificar a la misma mujer dentro de un universo de 2 mil personas en una comunidad, evidentemente estos datos no hacen identificable a nadie. A esta información se le denomina datos disociados porque han sido desvinculados de su titular y nunca será posible identificarlo con esfuerzos razonables.

Ejemplo de lo anterior son las estadísticas o los datos preliminares de los resultados en los procesos electorales; por ejemplo, en la elección del proceso electoral de 2012 para elegir a miembros de ayuntamientos e integrantes del Poder Legislativo en el Estado de México, el Padrón Electoral definitivo tenía registrados a 88 mil 581 hombres en el municipio de Lerma (IEEM, 2012). Con este dato si bien es cierto que es muy alta la posibilidad de que un vecino mayor de edad de ese municipio se encuentre registrado en el Padrón Electoral, el número total de ninguna manera nos permite identificar a los 88 mil 581 hombres registrados, mucho menos saber si cada individuo votó o no votó y por cuál partido lo hizo, aun consultando el porcentaje de votaciones por partido en la sección del municipio de Lerma en el Programa de Resultados Electorales Preliminares del Estado de México.

De dónde surge la necesidad de proteger los datos personales

A lo largo del tiempo y durante toda nuestra vida vamos dejando en diferentes lugares nuestros datos personales como parte de trámites y requisitos, sin pensar qué va a pasar con ellos cuando ya no sean necesarios o sin preocuparnos de si se van a transmitir mientras están vigentes. Sin embargo, ahora se reconoce la autodeterminación informativa, la posibilidad de decidir sobre nuestros datos personales. En el aún no tan lejano siglo pasado, nadie hablaba de la protección de datos personales en el país;[3] no obstante, en ese siglo comenzó a surgir la necesidad de protegerlos debido al rápido avance tecnológico, pues las computadoras, el Internet y la posibilidad de llevar y traer información en discos portátiles, ahora pequeñas memorias

[3] En Europa no fue así, pues es un tema que ha sido ampliamente abordado. Lo que existe en México ha sido tomado de la experiencia internacional, principalmente europea, en donde cuentan con disposiciones normativas relevantes al respecto y se reconoce la existencia de principios internacionales rectores de la protección de datos personales (que más adelante abordaremos).

portátiles, propició que enormes y pesados expedientes de datos personales se sintetizaran en bases de datos electrónicas fáciles de llevar y de enviar a lugares lejanos.

La sistematización da un alto valor a los datos personales. Un cúmulo enorme de hojas con información de las personas sin ningún aspecto en común identificado a nadie le sirve. Sin embargo, ya sea física o electrónica, aunque electrónica es mucho más fácil de utilizar y más valiosa por consiguiente, una base de datos con nombres y teléfonos de personas de la misma localidad con el interés común de participar en asuntos de su comunidad se vuelve muy valiosa para un partido político o para quienes pretenden integrar una asociación política o un nuevo partido. Principalmente, las bases de datos personales interesan a empresas con giros comerciales,[4] las que propiciaron un uso y transferencia indiscriminados de bases de datos personales; sin embargo, las bases de datos también son de gran interés para los partidos políticos.

El avance tecnológico ha favorecido la globalización y nos encontramos inmersos en una sociedad de la información que además de sus grandes ventajas, como el comercio y la circulación de información, también ha propiciado que poco a poco las personas vayamos perdiendo nuestra intimidad (Carranza, 2001, p. 19). Incluso debemos reconocer que en ciertas ocasiones es necesario ceder un poco de ésta en aras de ir adaptándonos a este avance tecnológico y generacional; por ejemplo, el uso de las videocámaras en los lugares que visitamos como medida de seguridad y el creciente uso de las redes sociales en nuestra vida diaria. De tal suerte que en Europa desde el siglo pasado se ocuparon de proteger la intimidad de las personas y de tratar de establecer mecanismos de control que impidieran el abuso en el uso y tratamiento de datos personales en perjuicio de la intimidad de las personas y su derecho a decidir sobre su información.

En México es un tema del cual apenas comenzamos a construir sobre bases firmes, pues antes del auge del derecho de acceso a la información sólo existían los abusos en el uso y transmisión de datos personales, incluso la venta de bases de datos, no olvidemos el famoso caso de

[4] Además del derecho de acceso a la información, otro de los aspectos que detonó en nuestro país la urgente necesidad de proteger los datos personales y legislar en la materia fue la cada vez creciente molestia que causaban los bancos a las personas al hacer llamadas telefónicas a los domicilios ofreciendo la venta de servicios o cobrando créditos vencidos. Esta última práctica después la continuaban empresas dedicadas a la recuperación de cartera vencida.

la empresa Choice Point, que afirmó haber obtenido el Padrón Electoral a través de la compra a una empresa privada (Redacción, 2010, párrs. 2-5).[5] Con la publicación de las primeras leyes de transparencia que permitían el acceso a la información en poder de instituciones públicas, fue necesario establecer ciertos límites a ese derecho de acceso, entre los cuales se previó una restricción a los datos personales, y de estas leyes viene la definición de dato personal; otro aspecto relevante fue la posibilidad de que las personas accedieran a sus datos a través de procedimientos sencillos establecidos en la ley, sin la necesidad de acreditar interés jurídico.

A partir de este momento se vuelve evidente la necesidad de un marco jurídico más amplio que garantice plenamente la autodeterminación informativa y conceda de manera clara los derechos de acceso, rectificación, cancelación y oposición de los datos personales, esto únicamente en cuanto a los datos personales en poder de instituciones públicas sujetas a leyes de transparencia.

Para adentrarse en el tema, la asistencia a eventos internacionales en Europa y países latinoamericanos, como Colombia o Argentina, permitió a los mexicanos hacer conciencia de la relevancia de la protección de datos personales, no sólo de aquéllos que se encuentran en archivos públicos, sino también de aquéllos en poder de particulares, respecto de los cuales no teníamos ninguna protección para evitar vernos vulnerados en nuestra vida íntima, domicilio, teléfono o simplemente en el derecho a estar solo.

La protección de datos personales

En México no existe una protección generalizada de los datos personales. De inicio, es necesario dividir la existencia de datos personales en instituciones públicas, las que están obligadas a las leyes de transparencia, y bases de datos que obren en archivos de particulares, las cuales se rigen por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010. Desde ahí es evidente que resulta complejo en México hablar de principios internacionales de protección de datos personales, pues la finalidad de establecer di-

[5] La nota periodística refiere que tres años antes de la elección presidencial de 2006 la empresa estadounidense Choice Point afirmó haber obtenido de manera legal el Padrón Electoral del Instituto Federal Electoral a través de la compra a una compañía mexicana establecida. Esta situación propició que en 2006 el Segundo Tribunal Unitario de Materia Penal de Primer Circuito clasificara este hecho como delito continuado de revelación de secreto.

chos principios es que los países los adopten en sus legislaciones para que exista una aplicación verdadera, incluso a través de la vía judicial.

En este sentido, si bien es cierto que las legislaciones nacionales aplicables a instituciones públicas e incluso directamente las que rigen a las autoridades en materia electoral no recogen por completo los principios internacionales propuestos por la Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad (Estándares Internacionales sobre Protección de Datos Personales y Privacidad, resolución de Madrid, 2009),[6] sí se parte de los principios más relevantes de este documento.[7] En Europa y otros países que están a la vanguardia en el tema pasa lo contrario, ya que se han tomado estos principios internacionales dándoles una forma doméstica o los han ampliado según sus criterios y necesidades.

Por lo anterior, en este apartado nos abocaremos a explicar los principios internacionales mínimos que debieran ser incluidos en las leyes de transparencia, en tanto no existan leyes de protección de datos personales aplicables a instituciones públicas.[8] Lo relevante es que aterrizaremos estos principios a la realidad de nuestro país, valorando primero el hecho de no contar con leyes de protección de datos personales en todos los estados, la convivencia del derecho de acceso a la información y el derecho de acceso y protección de datos personales, además de tomar en cuenta principios de derecho público, como aquél que dice que, *contrario sensu* al derecho civil, los servidores públicos (las autoridades electorales) no pueden hacer nada que no esté previamente establecido en la norma.

a. Principio de licitud. Un dato personal se recoge por una institución pública únicamente cuando se trata de información que sea necesaria para el desarrollo de sus funciones o cuando las personas requieren de un trámite o servicio prestado por el Estado. De tal suerte, un instituto electoral contará con la copia de la credencial de elector de todos aque-

[6] México no formó parte de los proponentes de esta resolución.
[7] La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en su artículo 6o., retoma ocho principios rectores de la protección de datos personales.
[8] Actualmente los estados de Colima, Guanajuato, México y Oaxaca, más el Distrito Federal, cuentan con leyes de protección de datos personales aplicables a instituciones públicas que sí abordan, aunque de manera indirecta, otros principios como licitud, consentimiento y proporcionalidad; además, el estado de Morelos en su ley de transparencia contempla de manera más amplia la protección de datos personales (véanse las leyes de transparencia o datos personales de los estados mencionados en la página del Instituto Federal de Acceso a la Información y Protección de Datos). Recientemente el Estado de México publicó en su *Gaceta del Gobierno*, el 31 de agosto de 2012 la LPDPEM, en donde también se retoman los principios internacionales de protección de datos personales.

llos ciudadanos que deseen ser registrados para contender por un cargo de elección popular. Esto es afín con las atribuciones que la Constitución y la ley específica otorgan a estas instituciones electorales; sin embargo, si dentro del país alguno de los institutos tomara la determinación de solicitar algún documento relacionado con los estados de salud de los aspirantes o el acta de nacimiento de sus hijos, evidentemente excedería de las atribuciones de las autoridades electorales, lo que constituiría una violación a la protección de datos personales. Para que una autoridad pueda llevar a cabo la recolección de un dato personal o aceptar que éstos le sean transmitidos, debe existir alguna disposición jurídica que lo autorice, ya sea de manera textual o que se desprenda de sus atribuciones; de otra forma la recolección de datos personales es ilegal.

b. Principio de información. Cuando se va a llevar a cabo una recolección, debe informarse previamente a las personas sobre los datos personales que serán recolectados; que existe la disposición jurídica que permite la recolección a la institución pública, en este caso a la autoridad electoral; el uso y destino que se dará a los datos personales; si es necesario hacer transmisiones a terceros; el plazo por el cual serán utilizados; los derechos que como titular de los datos personales se pueden ejercer y el nombre de la persona responsable de proteger los datos personales. Esta información debe entregarse en cada recolección de datos personales y constituye lo que poco a poco comenzamos a identificar como avisos de privacidad, obligatorios para los particulares, con las características propias que implica la naturaleza de cada actividad del ámbito privado.

Eventualmente pueden existir excepciones a este principio de publicidad, pues no necesariamente se contraviene. Se exceptúan aquellas transferencias que la institución pública por ley está obligada a realizar, como la entrega de datos de contribuyentes al Servicio de Administración Tributaria o a las instituciones de seguridad social, tampoco hay violación al principio de información cuando se entregan datos personales solicitados por autoridades judiciales o de procuración de justicia en ejercicio de sus atribuciones, pues aunque no se trate de una labor cotidiana, tratándo-

se de autoridades facultadas para acceder a esta información debe entregarse, en algunos casos bajo promesa de secreto. Esto se realiza sin que el titular de los datos se entere, para no ponerlo sobre aviso, por ejemplo, de la posible existencia de una investigación penal en su contra.

c. Principio de consentimiento. Las instituciones públicas requieren del consentimiento de las personas; es decir, éstas deben expresar la voluntad de entregar sus datos para que sean tratados por la institución dentro de sus atribuciones. El consentimiento debe otorgarse de manera informada, que sepan para qué se recolectan los datos, cómo y dónde serán utilizados, por quién y por cuánto tiempo (aviso de privacidad). La información debe proporcionarse antes de la entrega, la cual debe ser de manera libre, sin existir presiones y sin la posibilidad de equivocación en el consentimiento. Con el hecho de entregar los datos personales se puede reconocer la existencia de un consentimiento tácito, pero es importante dejar claro que el consentimiento también debe darse para el uso y tratamiento, incluida la transferencia a terceros si para cumplir el objetivo es necesaria.

d. Principio de finalidad. Este principio nos lleva a utilizar y a tratar los datos personales únicamente para cumplir con el objetivo propuesto, realizar un trámite o satisfacer un requisito. Retomando el ejemplo anterior, los datos personales de los aspirantes a ser registrados como candidatos no pueden utilizarse para un fin distinto o incompatible como entregarlos a una autoridad fiscal; sin embargo, si el fin fue la obtención del registro, pueden utilizarse para fines compatibles como una estadística para obtener un promedio de los hombres y mujeres que participaron y sus edades, pues esto encuentra relación directa con el fin principal y no existe una violación a la vida privada o a la intimidad de los ciudadanos, además son actividades acordes con la naturaleza de las autoridades responsables de organizar las elecciones.

e. Principio de proporcionalidad. Consiste en solicitar sólo aquellos datos necesarios para cumplir con la finalidad y que sean acordes con el objetivo por el cual se recaban; por ejemplo, un área administrativa encuentra justificación de solicitar un número importante de datos personales para integrar el expediente laboral

de todos sus trabajadores, como acta de nacimiento, de matrimonio o actas de nacimiento de los hijos, pues toda esta información guarda relación con el alta en las instituciones de seguridad social; sin embargo, aunque es proporcional solicitar al trabajador para el pago de la nómina mediante transferencia bancaria los datos de una cuenta, si además se requiere un estado de cuenta en donde sea visible el saldo del trabajador, evidentemente se solicita un dato desproporcionado con la finalidad que persigue un área administrativa.

f. Principio de responsabilidad. Consiste en brindar seguridad a los titulares de datos personales a través de designar a un servidor público directamente responsable del cuidado de estos datos, el cual puede ser contactado para tratar cualquier asunto relacionado con los mismos. Como complemento de sus obligaciones, la tarea de estos servidores públicos responsables debe sujetarse a políticas y medidas mínimas de seguridad de las bases de datos, las cuales deben hacerse del conocimiento público.

g. Principio de calidad. Los datos personales deben ser exactos y verídicos. Esto supone un deber de cuidado del servidor público responsable de la recolección o, en su caso, de la transmisión; es decir, se debe cuidar en todo momento que los datos estén libres de error y su debida actualización. En caso de detectarse datos equívocos, se deberá realizar la corrección respaldada con la documentación necesaria.

Existen más principios contemplados en los Estándares Internacionales sobre Protección de Datos Personales y Privacidad; sin embargo, podemos resumirlos en los aquí expuestos, principalmente porque están adecuados a nuestro contexto y al estrecho margen de actuación que nos permiten las incipientes leyes que regulan la materia. Así como se busca privilegiar su cumplimiento como mínimo para garantizar la autodeterminación informativa, también conviene destacar la existencia de excepciones, pues la protección de datos personales en archivos públicos, incluidos aquellos datos que obran en archivos de autoridades electorales, debe necesariamente convivir con el derecho de acceso a la información, rama del derecho que en su vertiginoso avance ha sentado criterios relevantes en beneficio de la transparencia y la rendición de cuentas.

Las excepciones que deben considerarse son únicamente en cuanto a la confidencialidad de los datos personales, pues en virtud de su relevancia en el ámbito del derecho público pierden esta protección de confidencialidad y se vuelven información pública, aunque esto no implica que deba omitirse su cuidado en la finalidad, calidad, proporcionalidad, responsabilidad, información y legalidad; sin embargo, no será necesario requerir el consentimiento para la publicidad. Como ejemplo de lo anterior, podemos mencionar los datos personales que acreditan el cumplimiento de disposiciones normativas (la edad del presidente de la República o del gobernador, porque es requisito constitucional tener una edad mínima para contender por estos cargos).

Lo mismo pasa con aquellos datos personales de servidores públicos que actúan en ejercicio de atribuciones (nombre, firma en todos los casos, número de cédula profesional y título cuando contar con éste sea un requisito para estar en condiciones de ejercer la profesión). También sucede con los datos personales que por disposición legal deben hacerse públicos (información pública oficiosa, como los sueldos de los servidores públicos). Estas excepciones no son arbitrarias, pues se han considerado en función de que es mejor para el interés público favorecer su transparencia que mantener su confidencialidad, lo que hemos comprobado en estos 10 años de vida que tiene la transparencia en nuestro país.

Marco normativo aplicable a los datos personales en el Estado de México

Derivado del auge que ha cobrado la protección de datos personales en nuestro país, primero existieron leyes de transparencia que previeron el derecho de acceso a los datos personales y su protección, posteriormente se reformaron los artículos 6o., 16 y 73 de la Constitución Política de los Estados Unidos Mexicanos. De estas reformas en realidad sólo impacta de forma directa a las instituciones públicas la del artículo 6o., en virtud de que el resto de las reformas estaban encaminadas a propiciar la aparición de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

El artículo 6o. de la Constitución se reformó el 20 de julio de 2007, con el fin de complementar en qué consiste el derecho de acceso a la información pública y especificar que “La información que se refiere a la vida privada y a los datos personales será

protegida en los términos y con las excepciones que fijen las leyes". Posteriormente, el 1o. de junio de 2009, se adicionó al artículo 16 constitucional lo siguiente:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Por último, el 30 de abril de 2009 se concedieron mediante una reforma constitucional atribuciones al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares.

La reforma al artículo 6o. de la Constitución federal generó reformas en todas las leyes de transparencia de las entidades federativas, para que, además del acceso a información pública bajo criterios mínimos, se tuviera derecho de acceder a los datos personales, siempre y cuando se fuera el titular de los mismos. Sin embargo, nos habiamos quedado cortos al no establecer legislaciones especializadas en datos personales, ya que nos provocó grandes problemas en la práctica no contar con leyes en las que se fundaran y motivaran de manera adecuada las determinaciones de los servidores públicos para proteger datos personales y la mayoría de las decisiones finales quedaban al arbitrio de la interpretación, claro está que esto no es óbice para que se realicen interpretaciones jurídicas con lo poco que las leyes nos proporcionaban.

Lo que también conviene destacar es que el artículo 16 de la Constitución sienta bases parciales de los que internacionalmente se identifican como derechos ARCO y aprovechamos este apartado para abundar en éstos. Se encuentran previstos en los Estándares Internacionales sobre Protección de Datos Personales y Privacidad (resolución de Madrid, 2009, parte IV); no son principios, sino, como su nombre lo indica, derechos de las personas que deben estar contenidos en la norma para cerrar el círculo virtuoso, pues son requisito *sine qua non* para garantizar la autodeterminación informativa.

a. Derecho de acceso. Consiste en garantizar a toda persona el acceso a sus datos personales. Esto puede implicar incluso que deban entregarse copias

certificadas, cuando no exista un trámite ex profeso para ello, con el objetivo de que el titular conozca los datos personales que obran en la institución pública y, en su caso, pueda advertir que son exactos y actuales. Este derecho al acceso se prevé en leyes de transparencia, pero debe dejarse claro que el objetivo es acceder a los datos personales como parte del derecho de autodeterminación informativa, no utilizarse como mesa de trámites de certificación, por lo que las legislaciones deben contemplar un límite al ejercicio reiterado de acceso a datos personales por plazos determinados.

b. Derecho de rectificación. Consiste en poder solicitar a la autoridad la corrección de los datos personales que obren en sus archivos y no sean exactos, así como establecer procedimientos para actualizarlos cuando sea necesario. Es importante acentuar que la carga de probar el error en los datos personales debe recaer siempre en el titular; esto es, sólo debe llevarse a cabo la corrección cuando acredite con documentos originales o copias certificadas que el dato es inexacto. La rectificación necesariamente debe implicar que el responsable de los datos personales notifique la modificación del dato o datos a todos los terceros a quienes se haya transmitido la información.

c. Derecho de cancelación. El objetivo de cancelar busca que una vez concluida o desaparecida la finalidad para la cual fueron recolectados los datos personales puedan ser dados de baja, lo que puede implicar destruirlos o, incluso, si se trata de documentos originales, devolverlos a su titular. El derecho de cancelación debe establecerse en ley bajo un procedimiento iniciado por el titular que permita suspender la posibilidad de cualquier uso por parte de la institución responsable, hasta que se verifique que ha concluido la finalidad o que se ha satisfecho y no existen disposiciones normativas que obliguen a la institución a mantener el dato por un plazo más amplio. Debe existir también la cancelación oficiosa por parte de las instituciones; de tal suerte que una vez identificado que la base de datos ya no se requiere y no hay restricciones jurídicas para su baja o destrucción, se lleve a cabo y se notifique a los titulares.

d. Derecho de oposición. Definitivamente en la práctica no existe en

nuestro país. Versa sobre conceder el derecho a las personas a no entregar sus datos personales, oponerse a la recolección, siempre y cuando exista alguna situación legítima del titular, la cual obviamente no puede darse cuando se trate de datos personales que deben entregarse en cumplimiento de disposiciones jurídicas, en cumplimiento de obligaciones o las realice la autoridad en ejercicio de sus atribuciones; por ejemplo, una persona no puede negarse a entregar su fecha de nacimiento (documento oficial en donde conste, como el acta de nacimiento), porque no desea que se revele su edad, si este dato es parte de los requisitos para obtener la credencial de elector.

Cerraremos este apartado centrándonos en la normatividad aplicable en el Estado de México, en donde se tardaron cinco años para aprobar la publicación de una ley especial. Por lo anterior, los servidores electorales durante este tiempo únicamente encontraron como marco de actuación la Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, publicada en la *Gaceta del Gobierno* el 30 de abril de 2004. Esta ley contempla la protección de datos personales al concederles en el artículo 25, fracción I, el carácter de confidenciales; además, establece en el artículo 25 bis el deber de todos los sujetos obligados al cumplimiento de esta ley de adoptar las medidas necesarias para garantizar la seguridad de los datos y evitar su pérdida, alteración o uso no autorizado. Por su parte, el artículo 26 señala que únicamente puede obligarse a las autoridades a entregar datos personales cuando se trate de asuntos de seguridad pública o para proteger la vida de las personas, siempre y cuando esta información no contenga datos que puedan generar discriminación.

Por último, dicha ley retoma los principios de calidad, finalidad, información y consentimiento, al determinar que los archivos con datos personales deben ser actualizados, utilizarse únicamente para los fines para los que fueron creados, tomarse medidas para informar a los titulares sobre su uso y no deben revelarse sin que exista el consentimiento del titular. Además, señala que los datos personales no deben exceder el plazo de la finalidad; no obstante, no se establecen procedimientos o reglas mínimas para cumplir con estos principios sucintamente previstos en la norma. En el rubro, existe un capítulo de acceso y corrección de datos personales, pero no para la oposición y cancelación. Esto era todo lo que existía legislativamente

para proteger los datos personales en el Estado de México. Posteriormente se publicó la LPDPEM donde se protegen los datos personales, aunque a la fecha no se le ha dado mucho auge.

La situación de los datos personales en el ámbito electoral y los criterios del Tribunal Electoral del Estado de México en materia de protección de datos personales

Lo que hemos explicado a lo largo del presente escrito, tanto lo que consta en ley como la aplicación de principios de protección de datos personales y derechos para garantizar a las personas la autodeterminación informativa, es algo que en la práctica del derecho electoral no se ha concretado. En realidad, los criterios de interpretación judicial se contraponen con la protección de datos personales, en aras de sobregarantizar derechos políticos. Los antecedentes planteados nos servirán para concluir con el análisis de un caso específico relacionado con la protección de datos personales.

El caso que se presenta, y que ha servido de base para resolver juicios similares, es el recurso de apelación RA/17/2011, el cual fue interpuesto por un partido político nacional ante el TEEM por la negativa del IEEM a entregar copias certificadas de documentos que contienen datos personales de ciudadanos —expedientes de registro de los ciudadanos que resultaron designados para ocupar cargos de instructores y capacitadores durante el proceso electoral 2011—. El partido político, a través de su representante propietario ante el Consejo Distrital número XXXII, requirió la entrega de la solicitud firmada, la declaratoria firmada, la fotocopia por ambos lados de la credencial de elector y la fotocopia del último certificado de estudios. Lo anterior, bajo el argumento de que se requerían para contar con los elementos objetivos suficientes que le permitieran a su integrante del Consejo Distrital Electoral intervenir en la organización, desarrollo y vigilancia de la elección de Gobernador e integrar los documentos que en su momento pudieran hacerse valer como elementos de prueba en el procedimiento de designación.

El Instituto Electoral del Estado de México, a través de su Consejo Distrital respectivo, determinó no entregar la información solicitada bajo el argumento de proteger los datos personales, con fundamento en los artículos 6o., fracción II, de la Constitución; artículo 5o., párrafos duodécimo a décimo cuarto y décimo quinto fracción II, de la Constitución

Política del Estado Libre y Soberano de México; así como en los artículos 1o., fracción V, inciso b; 2o., fracción II; 5o.; 8o.; 11; 19; 25, fracción I; y 25 bis, fracción I, de la Ley de Transparencia Estado de México, además del artículo 85 del Estatuto del Servicio Electoral Profesional. El argumento para negar la entrega se centró en la protección de los datos personales y en que el representante del partido político tenía derecho de acceso a los documentos sin que esto implicara la transmisión, además de que el procedimiento de designación incluye el Operativo para la Revisión de Expedientes de Aspirantes a Instructores y Capacitadores a los Cuarenta y Cinco Distritos Electorales, que le fue debidamente notificado.

Desde nuestra óptica, la respuesta del IEEM fue correcta, al valorar en su justa dimensión el acceso a datos personales desde el principio de finalidad, al determinar que no procede la transmisión de los datos personales. El cumplimiento de los derechos político-electorales de los partidos políticos a través de sus representantes se da a partir del acceso *in situ*, que se lleva a cabo en las reuniones en donde ellos pueden revisar y valorar si los aspirantes cumplen o no con los requisitos y, en dichas sesiones, hacer las manifestaciones o posiciones correspondientes, ya que la finalidad de la recolección de los datos personales es que todos los integrantes del Consejo Distrital los revisen, pero ello no implica que tengan derecho a llevárselos a su casa.

El aspecto negativo de la respuesta tiene que ver con el insistente señalamiento del derecho de acceso a la información, pues aunque éste como el de protección y acceso de datos personales se regían en 2011 por la misma ley, para el caso que nos ocupa no encuentran relación uno con otro, ya que se trata de derechos de distinta naturaleza y que se rigen por principios completamente opuestos. Esto es, el principio de máxima publicidad implica que cuando una institución pública tiene un documento debe privilegiar siempre su publicidad sobre la clasificación, pero aplica completamente lo contrario tratándose de datos personales, pues se debe privilegiar su confidencialidad, a menos que la publicidad del dato personal tenga un impacto directo en el interés público (esta valoración no se lleva a cabo en países que no se han desarrollado en derecho de acceso a la información, ya que siempre y en todos los casos los datos personales son confidenciales).

Es irrelevante si toda persona tiene derecho de acceso a los documentos públicos, ya que los datos perso-

nales no constituyen documentos públicos. Por otro lado, las reglas del derecho de acceso a la información pública no se aplican entre servidores públicos ni entre instituciones que actúan en ejercicio de sus atribuciones, sino por la legislación específica. No pasa lo mismo con los datos personales a los que sí aplican las reglas de protección entre servidores públicos y entre instituciones, ya que, por ejemplo, el área jurídica del IEEM no podría solicitar copias de las actas de nacimiento de todos los servidores electorales si no justificara que las requiere para el desempeño de sus obligaciones, o el Servicio de Administración Tributaria no puede solicitar datos personales de candidatos a cargos de elección popular porque no tiene atribuciones para ello, pero sí los puede solicitar de servidores electorales que son contribuyentes.

La determinación del TEEM consistió en revocar la respuesta del IEEM bajo el argumento de que a los representantes de los partidos políticos no los rige la Ley de Transparencia del Estado, lo cual es cierto de manera parcial, ya que en su calidad de integrantes de los consejos no requieren solicitar información pública bajo los procedimientos del derecho de acceso a información; sin embargo, sí aplicaba o debía aplicar la ley cuando se trataba de datos personales protegidos. Actualmente se debe atender a lo previsto en la ley específica. Toda vez que la información no es pública, existe un titular de la información con derecho a la autodeterminación informativa, la que se viola con la transmisión de sus datos personales. Además, el Tribunal determinó no valorar que los representantes de los partidos políticos tuvieron derecho de acceso a los documentos y a la revisión respectiva de éstos para verificar que los aspirantes cumplieran con los requisitos, en virtud de que ello no resolvía la solicitud de entrega de información en copias certificadas.

Se concluyó que el artículo 118 del Código Electoral del Estado de México no establece ningún límite para proveer o expedir información, documentación o copias certificadas. No se valoró que ningún derecho es ilimitado, pues cuando dos derechos se colisionan debe existir una valoración entre ambos para tomar la determinación más benéfica. En este caso se contraponen el derecho de un partido político a solicitar que le sean transmitidos datos personales frente al derecho de protección de datos personales y su confidencialidad, en perjuicio de los principios de finalidad, consentimiento, información y responsabilidad. Este

supuesto de colisión fue analizado por Manuel Atienza (2004) en un estudio distinto al que nos ocupa —bioética— pero relacionado con la privacidad.

> Cuando existe una contraposición entre la libertad de información[9] y el derecho a la intimidad: 1. Hay una presunción *prima facie* en favor del derecho a la intimidad. 2. Sin embargo, la libertad de información puede prevalecer si: 2.1 La información tiene relevancia pública 2.2. No contradice los usos sociales. (p. 64)

El Tribunal justificó la necesidad de la información con base en que el partido político requería contar con elementos objetivos para intervenir en la organización, desarrollo y vigilancia de la elección de Gobernador; sin embargo, se deja de lado que el procedimiento para la selección de instructores y capacitadores tiene una etapa en donde todos los integrantes tienen acceso a los documentos para verificar que los aspirantes cumplan con los requisitos y no se tomó en cuenta que como parte del Consejo Distrital tienen acceso a los documentos en todo momento. Argumentó también la necesidad de transmitir copias certificadas, aunque en realidad el ejercicio de sus atribuciones no se veía impedida, lo que daba como resultado que la transmisión no fuera requisito indispensable para vigilar el proceso de selección.

Encontraríamos justificada la necesidad si existiera un medio de impugnación por la designación de ciudadanos que no cumplen con los requisitos y la documentación se ofreciera como prueba. De lo contrario, si se afirma que sin la transmisión de copias certificadas se impide el ejercicio del derecho político-electoral de participar en las elecciones, se debe considerar que se violenta el derecho de todos los partidos políticos y de los ciudadanos consejeros al no disponerse la información en copias certificadas para cada uno, ello en función de la necesidad de realizar sus labores. Asimismo, existe plenamente un trato igualitario entre servidores electorales y partidos políticos. Bajo este supuesto tampoco los consejeros tendrían derecho a la transmisión de datos personales en copias certificadas, sólo de acceso a los expedientes.

Coincidimos plenamente con la afirmación de que los datos personales requeridos son los estrictamente

[9] En España no existe el derecho de acceso a la información, por lo que cuando Manuel Atienza se refiere a la libertad de información, debemos entenderlo en el sentido más amplio.

necesarios para verificar el cumplimiento de los requisitos; no obstante, se insiste en que fue excesiva la entrega en perjuicio de los ciudadanos, quienes desconocen que les fueron entregados sus documentos en copia certificada a los partidos políticos, y aunque éstos también están obligados a la secrecía de los datos personales y a utilizarlos con el único objetivo de verificar que los aspirantes cumplan con los requisitos, no existe ningún medio de control real para verificar esto y, en su caso, castigar cuando la secrecía o la falta de cuidado sea vulnerado; sin dejar de lado que la entrega no benefició al interés público, no obstante que los partidos políticos son entidades de interés público.

Asimismo, se violaron los principios de protección de datos personales; el de información, porque el TEEM no instruyó al IEEM para que notificara a los ciudadanos de que sus datos personales serían transmitidos a los partidos políticos —la recolección original no contemplaba la transmisión de los datos—; el de consentimiento, porque las autoridades no son propietarias de los datos personales y los ciudadanos tienen derecho a decidir si sus datos personales pueden ser transmitidos o no a terceros, por lo que, en todo caso, los ciudadanos tenían el derecho a no continuar con el proceso de selección si esta información tenía que ser transmitida a los partidos políticos, en garantía a la autodeterminación informativa; por último, se violó el principio de responsabilidad, ya que los procedimientos de protección no son aplicables en archivos de terceros, como los de los partidos políticos; además, actualmente ningún partido político garantiza la protección de datos personales, esto sin dejar de lado que entran en la regulación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Conclusiones

- El derecho de acceso a información pública y la protección a datos personales conviven en las mismas legislaciones debido al gran retraso que tenemos en México en materia de protección de datos personales; sin embargo, sus reglas son diferentes y sus principios filosóficos opuestos.

- Las autoridades electorales y los tribunales deben privilegiar en todo momento los derechos a la autodeterminación informativa y a la protección de datos personales, a menos que se demuestre que es mayor el beneficio al interés público.

Fuentes de consulta

Atienza, Manuel (2004). *Bioética, derecho y argumentación.* Bogotá: Themis.

Carranza Torres, Luis R. (2001). *Hábeas data. La protección jurídica de los datos personales.* Córdoba, Argentina: Alveroni Ediciones.

Constitución Política de los Estados Unidos Mexicanos. Recuperado el 17 de septiembre de 2012, de http://www.diputados.gob.mx/LeyesBiblio/pdf/1.pdf

Constitución Política del Estado Libre y Soberano de México. Recuperado el 17 de septiembre de 2012, de http://www.edomex.gob.mx/legistelfon/doc/pdf/ley/vig/leyvig001.pdf

Estándares Internacionales sobre Protección de Datos Personales y Privacidad, resolución de Madrid (2009). Recuperado el 10 de septiembre de 2012, de http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

Estatuto del Servicio Electoral Profesional. Recuperado el 18 de septiembre de 2012, disponible en www.ieem.org.mx

Instituto Electoral del Estado de México (2012a). Código Electoral del Estado de México. Recuperado el 19 de septiembre de 2012, de http://www.ieem.org.mx/transparencia/pdf/fraccionI/codigos/04_CEEM12.pdf

Instituto Electoral del Estado de México (2012b). Registro Federal de Electores por Distrito Local y Sexo Definitivo para la Elección del 1 de julio de 2012. Recuperado el 5 de septiembre de 2012, de http://www.ieem.org.mx/numeralia/lista_nominal.html

Instituto Federal de Acceso a la Información Pública y Datos Personales (2012). Recuperado el 13 de septiembre de 2012, disponible en http://www.ifai.org.mx/

Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios. Recuperado el 17 de septiembre de 2012, de http://www.edomex.gob.mx/legistelfon/doc/pdf/ley/vig/leyvig094.pdf

Recurso de apelación RA/17/2011 del Tribunal Electoral del Estado de México. Recuperado el 20 de

septiembre de 2012, disponible en http://www.teemmx.org.mx/.

Redacción (2010, 21 de abril). "Tráfico de datos sigue, a 7 años de Choice Point". *El Universal.* Recuperado el 18 de septiembre de 2012, de http://www.eluniversal.com.mx/notas/674394.html.

Sánchez Montenegro, Héctor (Coord.) (2009). *La protección de datos personales. Soluciones en entornos Microsoft.* Madrid: Agencia Española de Protección de Datos/Ministerio de Industria, Turismo y Comercio.