La credencial para votar y la protección de los datos personales

Delia Matilde Ferreira Rubio

Sumario: I. Conflicto de fondo; II. Sentencia y decisiones posteriores; III. Datos personales. Registro, tratamiento, constancia y difusión; IV. Valoración de la solución adoptada, V. Fuentes consultadas.

I. Conflicto de fondo

La protección de los datos personales ha sido una preocupación en la agenda pública latinoamericana, en particular en los últimos 15 años, en conexión —en muchos países— con la búsqueda de garantizar el derecho de acceso a la información pública. La primera ley de protección de datos en la región fue la Ley argentina 25.326 de 2000.[1] En la actualidad Brasil, Bolivia, Chile, Colombia, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Perú, Panamá, Paraguay, República Dominicana, Uruguay y Venezuela cuentan también con normas —de rango constitucional o de ley— de protección de datos personales (Remolina 2014).

[1] El texto de la Ley 25.326 puede consultarse en http://www.jus.gob.ar/media/33481/ley_25326.pdf. En Europa y Estados Unidos las primeras leyes de acceso a la información y protección de datos personales se remontan a la década de 1970. La primera ley fue la del estado de Hesse, en Alemania, de 1970. Al respecto, véase Jóri (2007), en especial, el capítulo 3.

El disparador central de la preocupación por la protección de los datos personales ha sido el desarrollo de las tecnologías de la información, que hoy en día permiten el cruce de datos y el acceso a ellos con gran facilidad y rapidez, y los controles característicos de la era preinformática o preinternet no son eficientes o adecuados para impedir abusos.

La protección de la vida privada o la intimidad ha sido una constante en la legislación, desde el derecho romano hasta la actualidad, pero ha sido necesario cambiar y ampliar esa protección a medida que la tecnología ha facilitado nuevas formas de intromisión. Siglos atrás bastaba la protección física del domicilio o de la correspondencia. Luego aparecieron la fotografía, la grabación de voz y, recientemente, la acumulación de datos en registros de fácil acceso (Ferreira 1982), y con estos desarrollos tecnológicos surgió la necesidad de prever nuevas medidas jurídicas de protección (Bustillos 2011, 317-46).

El conflicto al que se refiere la sentencia que se comenta se relaciona con un dato personal en particular: el domicilio, que no solo forma parte de la información de rastreo y ubicación de una persona, sino que es considerado —desde el derecho romano— como un atributo de la personalidad. ¿Se puede hacer público el domicilio en un instrumento emitido por el Estado, como la cédula para votar? Tradicionalmente había sido así en muchos de los países de América Latina, y la cuestión no había generado mayores debates o planteos.

En la actualidad, el tema despierta inquietud en parte por razones jurídicas y en parte por el contexto social en el que se vive. En cuanto a las razones jurídicas, en el caso de la sentencia que se comenta, el problema se plantea porque las normas de protección de datos personales establecen que estos tienen el carácter de confidenciales, y entre ellos se incluye el domicilio de una persona, pero las normas electorales disponen que el documento habilitante para votar —la credencial para votar— debe contener el domicilio.

A este conflicto jurídico se suman consideraciones prácticas que también deben ser tenidas en cuenta y que dividen la opinión de la ciudadanía. Entre dichos factores prácticos o funcionales, la inclusión del domicilio puede facilitar la realización de trámites en los que es necesario acreditarlo. Por otro lado, en contextos de violencia e inseguridad, la inclusión del

domicilio de la persona en un documento puede traer problemas de gravedad en caso de robo o pérdida.

Este es el conflicto que constituye el nudo de la discusión en este caso. La sentencia de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación (TEPJF) y las decisiones a las que dio lugar han contribuido a dar una solución satisfactoria al problema. En efecto, a la sentencia que se comenta siguió la revisión del acuerdo del entonces Instituto Federal Electoral (IFE) —hoy Instituto Nacional Electoral (INE)—, que decidió que al momento de la tramitación de la credencial para votar sea el ciudadano el que decida la forma en que el domicilio constará en el documento, ya sea en forma visible —como había sido habitual—, ya sea en forma encriptada. Esta última decisión fue avalada por el propio Tribunal en su sentencia SUP-RAP-182/2013 en enero de 2014.

Las sentencias de los tribunales pueden ser analizadas desde distintos puntos de vista y diversos ángulos jurídicos y legales. Muchas de las consideraciones de la sentencia que se comenta tienen que ver con cuestiones procesales o de procedimiento específicas del derecho mexicano, que no se abordarán en este comentario, que estará centrado en los aspectos relacionados con el conflicto de fondo: la forma en que el domicilio —dato personal confidencial— debe aparecer en la credencial para votar.

II. Sentencia y decisiones posteriores

Decisión cuestionada

La sentencia dictada el 29 de mayo de 2013 por la Sala Superior del TEPJF (SUP-RAP-37/2013) resovió la impugnación interpuesta por el Partido Acción Nacional (PAN) contra el acuerdo CG84/2013 del Consejo General del entonces IFE adoptado en la sesión del 27 de febrero de 2013.

En 2012 el IFE decidió modificar el modelo de la credencial para votar y encargó a la Dirección Ejecutiva del Registro Federal de Electores la realización de un estudio técnico específico en relación con la

viabilidad de incluir el domicilio del ciudadano en forma visible en la credencial para votar (acuerdos CG732/2012 y CG733/2012, respectivamente).

El acuerdo CG84/2013 disponía "mantener los datos de calle, número exterior y número interior del domicilio de los ciudadanos, de manera visible en la Credencial para Votar" (artículo 1).

Para adoptar la resolución acerca de la inclusión del domicilio en forma visible en la cédula para votar, el Consejo General del IFE tomó en cuenta los resultados de una encuesta nacional y de una encuesta abierta en línea, así como los resultados de una serie de consultas a organismos públicos y privados, al Instituto Federal de Acceso a la Información y Protección de Datos (Ifai) y a expertos en el tema.

La encuesta nacional reflejó una preferencia mayoritaria de los ciudadanos en favor de la inclusión del domicilio completo en forma visible en la credencial para votar. El total de apoyo fue de 49.7%, mientras que en las áreas no urbanas el número se elevó a 67 por ciento. Evidentemente, esto se vincula con la utilización práctica de la cédula para votar y así surge de la propia encuesta. Entre los fundamentos de su preferencia, los consultados mencionaron que el domicilio visible en la credencial es útil para realizar trámites, acreditar la identidad, poder avisar en caso de emergencias y acreditar la residencia; 32.2% de los encuestados prefirió la opción de ocultar los datos de domicilio.

Los datos de la consulta abierta en línea arrojaron un resultado distinto: 57% de los más de 5,000 participantes estuvo a favor de la inclusión del dato en forma cifrada o codificada, no accesible a simple vista.

De las 134 instituciones públicas y privadas consultadas, 42 dijeron que utilizan los datos de domicilio que figuran en la cédula para votar como información para la realización de diversos trámites administrativos. De estas 42, 24 instituciones respondieron que si el domicilio no figuraba en forma visible podrían implementar mecanismos tecnológicos para leer la información cifrada. Las 18 restantes contestaron que no estaban dispuestas a recurrir a herramientas tecnológicas para leer la parte cifrada de la credencial si el domicilio no estaba visible.

Dado que México cuenta con una legislación específica para la protección de datos personales y ha creado un organismo especializado en

la materia —el Ifai—, la opinión de este es de gran peso en la cuestión. En los fundamentos del acuerdo CG84/2013 se afirma al respecto que

> El Instituto Federal de Acceso a la Información y Protección de Datos consideró que la inclusión visible de los datos de la calle, número exterior y número interior en la Credencial para Votar no pone en riesgo la protección de los datos personales del ciudadano, "en tanto se genere para el ciudadano información suficiente sobre la importancia de los datos ahí contenidos para que estos adopten ciertas medidas elementales de cuidado y en tanto se propicie una cultura de cuidado responsable para toda persona que en el desarrollo de actividades legitimas posea datos de la credencial para votar".

Finalmente, el Consejo General del IFE entendió que la inclusión visible del domicilio en la credencial para votar era necesaria para que se llevaran a cabo las actividades de notificación, visita y capacitación de los ciudadanos designados para cumplir funciones en el proceso electoral.

Argumentos de la impugnación

El PAN impugnó el acuerdo el 5 de marzo de 2013 y el 11 de marzo el representante del Partido de la Revolución Democrática (PRD) presentó un escrito como tercero interesado. Cabe recordar, como deja claro el Tribunal en la sentencia, que el tercero interesado contradice la pretensión del apelante y su interés es el de mantener vigente el acto cuestionado. En síntesis, en cuanto al conflicto de fondo, el PAN estaba en desacuerdo con que el domicilio del ciudadano figurara en forma visible en la credencial para votar, mientras que el PRD estaba a favor de mantener esa información visible, tal como había decidido el Consejo General del IFE.

La impugnación del PAN se sostiene en su calidad de entidad de interés público, que le permite actuar en defensa del interés público, colectivo y difuso cuando considere que se ha violado el principio de legalidad, como

reconoce el Tribunal en el considerando segundo, punto d, de la sentencia que se comenta.

Los cuestionamientos al acuerdo CG84/2013 se basaron en argumentos de procedimiento y argumentos de fondo. Desde el punto de vista del procedimiento, el PAN cuestiona el acuerdo por estar deficientemente fundado y motivado. El agravio de fondo que esgrime el PAN se refiere a que el acuerdo violaría el derecho de las personas a la protección de sus datos personales, derecho amparado tanto en el ámbito constitucional como legislativo.

Para el PAN, el estudio técnico que incluyó la realización de la encuesta nacional y las consultas referidas más arriba resulta insuficiente, lo que determina que el acuerdo no está debidamente fundado y motivado. El PAN hace hincapié en la respuesta del Ifai que, si bien indicó que "en general" la visibilidad del domicilio en la credencial para votar no afecta la protección de los datos reservados, agregó que ello era así siempre que se dieran tres condiciones:

1) Que se instruya al ciudadano acerca de la importancia del dato incluido en la credencial y la necesidad de que adopte medidas de cuidado al usarla.
2) Que se construya una cultura de cuidado del uso de la credencial.
3) Que se faciliten al ciudadano mecanismos para la protección de su información personal.

La interpretación del PAN de la respuesta del Ifai es que, dado que esa cultura de cuidado de los datos personales no existe aún, la inclusión del domicilio en forma visible sí presenta riesgos para la protección de los datos personales.

El PAN resalta que, en su respuesta a la consulta del IFE, el Ifai se refiere al cumplimiento del artículo 20 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), que dispone la obligación de los sujetos responsables de bases de datos y registros de datos personales de tratar los datos solo cuando "sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido". Adecuación, pertinencia y no

exceso son los criterios que deben guiar el "tratamiento de datos", es decir, su utilización, cruce, distribución, ordenamiento y clasificación.

El PAN aduce que el estudio técnico debió analizar la inclusión del domicilio en forma visible, a la luz del principio de protección constitucional del derecho a la protección de los datos personales y de los tres criterios establecidos en la LFTAIPG, así como de los principios generales aplicables a la cuestión: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. En la medida en que este análisis no figura en los antecedentes, el acuerdo está insuficientemente motivado.

Otra línea argumental del PAN se relaciona con los efectos de la no inclusión del domicilio en forma visible en la credencial para votar para las tareas de notificación y capacitación de los ciudadanos que lleva a cabo el IFE. El PAN afirma, con razón, que el IFE cuenta con la información de localización de los ciudadanos en sus registros y no necesita ponerla en forma visible en la credencial para acceder a ella. En efecto, los organismos pertinentes del IFE pueden consultar las bases de datos de electores y utilizar su domicilio para notificarlos o localizarlos a fin de capacitarlos. Surge aquí una distinción importante respecto de la función de la credencial, que es la de identificación, no la de localización o georreferenciación del ciudadano.

En cuanto a las entidades consultadas, el PAN señala que se debió recurrir a la Comisión Nacional Bancaria, como organismo regulador, y no a los bancos o las entidades intermedias que los nuclean. Más allá de cuáles sean las prácticas en algunos bancos, el PAN resalta que la legislación no incluye a la credencial para votar como comprobante válido para acreditar el domicilio. Por lo tanto, la inclusión visible de este dato personal resulta absolutamente irrelevante desde el punto de vista bancario.

El PAN cuestiona asimismo que el estudio técnico no haya dado suficiente importancia a la opinión emitida por la Secretaría de la Defensa Nacional, en el sentido de que la inclusión cifrada o codificada del domicilio en la credencial para votar estaría en coincidencia con la política de seguridad adoptada por el Estado.

Otro argumento que fundamenta la impugnación es que el estudio técnico no analiza si la encriptación o codificación del domicilio afecta

algún derecho —más allá de la opinión o las preferencias subjetivas de los ciudadanos—.

La credencial para votar cumple dos funciones primordiales: habilitar al elector para votar y acreditar la identidad del elector. Para ninguna de estas funciones hace falta que el domicilio aparezca en forma visible. Además, y hasta que se emita la cédula de identidad, la credencial para votar puede servir como medio de identificación personal para trámites administrativos. El domicilio no forma parte de la identidad de la persona, por lo tanto, tampoco esta función justificaría la necesidad de que figure en forma visible en el documento.

Para el PAN, puesto que el domicilio es un dato confidencial, no debería figurar en forma visible en la credencial. El IFE aprobó oportunamente los Lineamientos de Protección de Datos Personales que establecen los principios que deben regir el tratamiento de los datos personales. Dichos principios son los de licitud, finalidad y proporcionalidad, calidad y seguridad. Supuestamente, incluir el domicilio en forma visible contradice el principio de seguridad en el tratamiento de datos. El principio de seguridad exige que se adopten

> las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.

Criterio del Tribunal y la resolución

La Sala Superior del TEPJF resolvió revocar el acuerdo CG84/2013, a efecto de que el IFE realizara una valoración ponderada de los argumentos a favor y en contra de la inclusión en forma visible del domicilio en la credencial para votar y evaluara la posibilidad de que el ciudadano —en ejercicio del derecho a la autodeterminación informativa— optara por la visibilidad o encriptación del domicilio en dicho documento.

En cuanto a la deficiente motivación del acuerdo cuestionado, siguiendo la jurisprudencia del propio Tribunal, la Sala Superior recordó que

> tratándose de los acuerdos generales que emite la autoridad electoral, los requisitos de fundamentación y motivación se satisfacen bajo premisas distintas a las que se requieren para otros actos de autoridad, porque en estos casos, al tratarse del despliegue de su potestad reglamentaria, basta que tenga reconocida en la ley la facultad para emitirlos en la materia relativa y los pronuncie apegados a la legalidad.

Conforme a esta orientación, el Tribunal considera en su sentencia que el IFE tiene competencia para emitir la credencial y determinar su formato, con lo cual estarían satisfechos los requisitos de fundamentación y motivación. Sin embargo, para la Sala Superior "el acuerdo impugnado […] examinado de manera integral en estricto sentido desatiende el mandato de la debida motivación" por dos razones:

1) En el acuerdo impugnado se exponen suficientemente los argumentos a favor de la visibilidad del domicilio en la credencial para votar, pero no se aclaran los argumentos por los que se desestima de la opción opuesta, es decir, la incorporación de los datos en forma codificada o encriptada. Aunque esto parezca un juego de palabras, en síntesis, la sentencia sostiene que el acuerdo explica por qué está a favor de la visibilidad del domicilio pero le falta explicar por qué está en contra de la encriptación del dato.
2) En el acuerdo impugnado no se consideró la posibilidad —propuesta por el PAN— de dar al ciudadano la opción de elegir entre la inclusión del domicilio en forma visible o en forma codificada, opción que se basa en la autodeterminación informativa, derecho consagrado en materia de protección de datos personales.

En cuanto a la necesaria protección de los datos personales, como el domicilio, el Tribunal destacó la legitimidad del IFE para colectar la información del domicilio de los ciudadanos como un elemento central para determinar dónde les corresponde votar, lo que contribuye a la certeza y credibilidad del proceso electoral. Asimismo, destacó que la normativa que regula la credencial para votar establece que el domicilio es uno de los contenidos mínimos que debe comprender

el documento, conforme al artículo 200 del Código Federal de Instituciones y Procedimientos Electorales.

Uno de los fundamentos del acuerdo cuestionado se refiere a la estrategia del IFE de consolidar la credencial para votar como documento de identidad, para lo cual el IFE consideró útil incluir el domicilio en forma visible. Con respecto a este argumento, el Tribunal recuerda que la normativa acerca de la cédula de identidad —cuando se emita efectivamente— no exige que esta contenga el domicilio —ni visible ni encriptado—. Por lo tanto, aunque no se incluya el domicilio en forma visible, la credencial para votar podrá seguir siendo utilizada como forma de identificación para trámites administrativos, conforme al artículo cuarto transitorio del decreto de modificación de la Ley General de Población.

Lo que se discute en el caso es quién tiene control de los datos personales que se consideran confidenciales. En este punto entra en juego el derecho de autodeterminación informativa —reconocido constitucionalmente en México—, que es la facultad de cada persona de controlar el flujo de información de los datos que hacen a su vida privada. Las personas tienen derecho a saber qué datos personales poseen las autoridades públicas o los bancos de datos privados, a exigir la rectificación de la información cuando sea incorrecta y a decidir quién puede acceder a esos datos en tanto información individual.

Como recuerda el Tribunal, la protección de los datos personales tiene rango constitucional en México. En efecto, el artículo 6-II de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) dispone que "la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes". En la misma dirección, el párrafo adicionado en 2009 al artículo 16 de CPEUM estableció con más detalle cuáles son los derechos de las personas sobre los datos personales en poder de entidades públicas o privadas:

> 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 deter-

minará los supuestos de excepción a los principios que rijan el tratamiento de datos.

Estos derechos son expresión del principio de autodeterminación informativa.

El Tribunal también destaca que la protección constitucional de la intimidad y los datos personales se instrumenta en el ámbito legislativo por medio de la LFTAIPG, que define qué debe entenderse por datos personales. El Tribunal sostiene que

> la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, tutela el derecho a la protección de datos personales de las personas físicas, y se encauza al respeto del derecho personalísimo de la intimidad, así como al de su confidencialidad, en los términos siguientes: Artículo 3. Para los efectos de esta Ley se entenderá por: […] II. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad (sic) (SUP-RAP-37/2013, 64).

Llama la atención, sin embargo, que al citar el artículo 3 de dicha ley, el Tribunal reproduzca un texto que no es el vigente. En efecto, en 2010 la definición de datos personales fue modificada y se eliminó la enumeración que es clave en el caso que se considera. El texto vigente del artículo 3-II de la LFTAIPG define los datos personales como "la información concerniente a una persona física, identificada o identificable".[2]

Dichos datos personales se consideran confidenciales cuando su difusión requiera del consentimiento de los individuos, y la LFTAIPG, en el artículo 21, aclara que

[2] Fracción reformada DOF 05-07-2010. Acerca de la evolución de las modificaciones a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, véase LFTAIPG.

> Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso […] de los individuos a que haga referencia la información.

Esta obligación de tratamiento confidencial de los datos personales está avalada por una serie de normas que el Tribunal repasa cuidadosamente. Entre estas, el Código Federal de Instituciones y Procedimientos Electorales, en el artículo 171, inciso 3, dispone expresamente que "los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores […] serán estrictamente confidenciales y no podrán comunicarse o darse a conocer", salvo en los casos de excepción previstos.

Ahora bien, dichas normas se refieren al tratamiento de los datos personales por parte de los organismos oficiales. A juicio de quien esto escribe, entregarle a una persona un documento oficial en el que aparece su propio domicilio no implica difundir, distribuir ni comercializar el dato privado (se retomará el particular en el siguiente apartado.)

Un principio rector de la interpretación de las normas de derechos es el principio propersona, que obliga a interpretar las reglas de la forma más favorable a las personas, promoviendo el respeto, protección y garantía de los derechos con atención de los criterios de universalidad, interdependencia, indivisibilidad y progresividad. El Tribunal entiende que el IFE debió realizar un ejercicio de ponderación con base en estos criterios antes de decidir acerca de la visibilidad o no del domicilio en la credencial para votar. Esta ponderación entre la utilidad de la inclusión visible del dato y la necesidad de proteger la confidencialidad del dato personal hubiera dado sustento efectivo a la decisión, pero no se llevó a cabo.

Estos argumentos y razonamientos llevaron al Tribunal a revocar la decisión y exhortar al IFE para que realizara la correspondiente ponderación de los derechos en juego y evaluara la opción de dejar la decisión acerca de la visibilidad del domicilio en manos de cada persona.

¿Qué sucedió después de la sentencia?

En cumplimiento de la decisión del Tribunal, el IFE ordenó realizar la ponderación solicitada y analizar y evaluar la posibilidad de que la forma en que el domicilio aparecerá en la credencial para votar dependa de la decisión de cada ciudadano.

El 23 de octubre de 2013, por medio del acuerdo CG292/2013, el IFE resolvió modificar la decisión original y estableció la obligación de consultar a los ciudadanos de forma expresa y por escrito acerca de la incorporación visible de los datos de domicilio en el anverso de la credencial para votar. El acuerdo dispone que, en todos los casos y con independencia de la decisión de cada persona, el domicilio figurará en forma encriptada en el reverso de la credencial.

En los fundamentos del acuerdo CG292/2013 se reconoce que —luego de realizar la ponderación que solicitó la Sala Superior del TEPJF— queda claro que no hay ningún impedimento legal para que el domicilio figure en forma codificada o cifrada en la credencial para votar y que la no visibilidad del domicilio en dicha credencial no afecta su utilidad para el fin principal al cual está destinada: la identificación de la persona y la habilitación del voto.

Pero la historia no había terminado aún. En diciembre de 2013, el PRD y el Partido del Trabajo impugnaron el nuevo acuerdo, aduciendo falta de motivación y violación de normas constitucionales y legales, ya que —entendían— la no inclusión del domicilio en forma visible atentaba contra la seguridad y certeza del sufragio. El Tribunal resolvió —en el expediente SUP-RAP-182/2013— ratificar el acuerdo CG292/2013, que consideró suficientemente motivado y congruente con la sentencia anterior de la Sala Superior acerca de la cuestión.

El procedimiento de consultarle al ciudadano, cuando tramita la credencial para votar, si desea que su domicilio figure en forma visible en el anverso del documento se puso en marcha a principios de 2014. Hasta el mes de mayo de 2014, de un total de más de cinco millones de ciudadanos que tramitaron la credencial para votar, solo 8% había optado por la encriptación del dato del domicilio. La cifra, según declaraciones del consejero José Roberto Ruiz, es inferior a lo que

se esperaba (Crónica). Aunque, a decir verdad, la preferencia de los ciudadanos parece congruente con los resultados de la encuesta nacional antes mencionados y que el IFE había tomado en cuenta para decidirse —en el acuerdo CG84/2013— por la visibilidad del domicilio en la credencial.

III. Datos personales. Registro, tratamiento, constancia y difusión

La protección de los datos personales y la garantía de la autodeterminación informativa son manifestaciones de la protección del derecho a la vida privada o derecho a la intimidad. La concepción del derecho a la privacidad —al igual que el conjunto de datos, hechos o situaciones protegidos— ha variado con el paso del tiempo, no solo en función de la aparición de nuevas formas de ataque, sino también, y fundamentalmente, a medida que se modifican las ideas y valoraciones sociales (Cifuentes 2008, 582-702) acerca de la relación entre lo público y lo privado y la función del Estado y el derecho de los ciudadanos a mantener un control de la administración.

Así, se pasó de una concepción del derecho a la intimidad centrada solo en la noción restrictiva del derecho a ser dejado en paz a la idea de garantizar la libertad de pensamiento y acción de la persona, para finalmente incorporar el derecho de autodeterminación informativa o control de la propia información (Rodotá 1983, 186-93). Todas estas facetas integran hoy el concepto de derecho a la privacidad y cada una supone una serie de garantías y herramientas jurídicas de protección. Tradicionalmente, el derecho a la reserva de la vida privada fue garantizado por medio de la consagración de la inviolabilidad de la correspondencia y del domicilio —entendido como el ámbito físico de residencia y no como simple dirección—. Pero esa protección ya no es suficiente.[3]

En la sociedad de la información, cuando existe una inmensa cantidad de información personal en manos del Estado y de organizaciones

[3] Acerca de la situación en América Latina, véase Zamudio (2012, 2-21).

privadas y la tecnología facilita el cruce de información en cuestión de segundos, se han hecho necesarios otros procedimientos de garantía (Alvarez-Cienfuegos 1999), no solo de exclusión de terceros, sino con herramientas proactivas para que las personas puedan retomar el control de su información personal. El derecho a la autodeterminación informativa (Hassemer y Chirino 1997) solo puede hacerse efectivo si se otorga a la persona la capacidad de acceder a la información contenida en los bancos de datos y registros, solicitar la rectificación si esa información es errónea, pedir la cancelación del registro en los casos en que la información sea improcedente, y oponerse a la recolección y tratamiento de algunos datos. Estas facultades son conocidas como derechos arco. El Reglamento de Transparencia del INE, según la modificación aprobada en julio de 2014, contempla estos derechos en el artículo 2-XIX.

Una muestra clara de la continua evolución y revisión del ámbito de protección del derecho a la intimidad es la actual discusión acerca de "el derecho a ser olvidado", que se debate en el contexto de la protección de la información personal que circula en internet, cuyo acceso se ha potenciado con la aplicación de los motores de búsqueda en la red. Aunque la discusión es reciente, ya ha dado lugar a fallos, como el de la Corte de Justicia de la Unión Europea en un caso contra Google. El derecho al olvido sería un corolario de lo que se conoce como privacidad digital.[4]

El objetivo de la protección de los datos personales puede ser resguardar la intimidad de la persona, su tranquilidad y la no perturbación de su espacio de reserva, que es el espacio de libertad. La persona decide con quién compartir esta información. Otras veces se protegen dichos datos para evitar persecuciones o discriminaciones (Guerra 2011, 103), especialmente cuando se reconoce el carácter sensible o confidencial de datos acerca de ideas políticas o creencias religiosas.

Pero qué información queda comprendida bajo ese paraguas es una cuestión que no tiene una respuesta universal, porque depende de la idiosincrasia y la cultura, y también de la posición y función que ocupan los diversos actores sociales (Shattuck 1977; Ferreira 1982).

[4] Sobre privacidad digital, véase la resolución que aprobó Naciones Unidas en noviembre de 2014 (ONU 2014).

Por lo tanto, los aspectos comprendidos en la protección de la vida privada o intimidad varían de una sociedad a otra y de un momento histórico a otro.

Hoy en día hay consenso más o menos generalizado acerca de algunos aspectos que integran la zona protegida, como la salud, los afectos, la filiación y las relaciones de parentesco, las preferencias sexuales, y las creencias ideológicas y religiosas. En cambio, se discute la inclusión de datos acerca de la situación económica de una persona, la vida profesional, y los entretenimientos y diversiones (Ferreira 1999, 129-43). La labor jurisprudencial en cada país ha sido de fundamental importancia para perfilar los contornos de la zona de reserva o protección de la vida privada.

La respuesta que se dé a la pregunta anterior tendrá reflejo en la definición de datos personales y en la protección que se les asigne.[5] Por eso, en algunas legislaciones se distingue entre datos personales y datos sensibles, una subespecie que merece una protección especial (Lavalle 2009).

En la Ley de Protección de Datos Personales en Posesión de Particulares se adopta esta diferenciación. En el artículo 3-V se definen los datos personales como "cualquier información concerniente a una persona física identificada o identificable", y en el punto VI del mismo artículo se definen los datos personales sensibles como

> 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.

Como se señala en el apartado anterior, llama la atención que el Tribunal cite en los fundamentos de la sentencia que se comenta un

[5] Al respecto, véase Directiva 95/46/CE del Parlamento Europeo (1995).

texto de la Ley de Transparencia y Acceso a la Información Pública Gubernamental ya derogado. Hasta 2010, la definición de datos personales del artículo 3-II era la que cita el Tribunal:

> La información concerniente a una persona física, identificada o identificable, entre otra la relativa a su origen étnico o racial, o que está referida a las características, físicas, morales o emocionales, su vida afectiva y familiar, domicilio […], *número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales,* o otras análogas que afecten su intimidad.[6]

Este artículo zanjaba claramente la discusión acerca de si el domicilio era o no un dato personal. En efecto, por disposición de la ley, lo era.

En 2010 el artículo fue modificado y el texto vigente define los datos personales como "cualquier información concerniente a una persona física identificada o identificable". La enumeración que cita el Tribunal ya no está en la Ley de Transparencia.

La mención original del domicilio entre los datos personales sin duda influyó en la conceptualización de reglamentos y lineamientos acerca de acceso a la información pública elaborados por diferentes organismos públicos mexicanos, aun cuando la ley fuera posterior y se optara por una conceptualización genérica.

Para el caso que aquí ocupa, el Reglamento del Instituto Nacional Electoral en materia de Transparencia y Acceso a la Información Pública (INE/CG70/2014) —cuya modificación fue aprobada el 2 de julio de 2014— reproduce aquella definición original en el artículo 2-XVII, al definir datos personales como

> la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las físicas, morales o emocionales, a su vida afectiva y familiar, domicilio […], número telefónico, patrimonio, ideología y opiniones

[6] Fracción reformada DOF 05-07-2010. La evolución de las modificaciones a la ley pueden consultarse en LFTAIPG.

> políticas, creencias o convicciones religiosas o filosóficas, el estado de salud físico o mental, las preferencias sexuales, u otras análogas que afecten su intimidad.

La protección de los datos personales así entendidos se completa con lo dispuesto en el artículo 35-1 del Reglamento: "los datos personales son información confidencial que no puede otorgarse a persona distinta de su titular, a menos que exista una autorización expresa de éste". En el mismo sentido, los Lineamientos Generales para la Clasificación y Desclasificación de la Información del IFE, en el artículo 28, disponen que "será confidencial la información que contenga datos personales de una persona física identificada o identificable relativos a: […] VII. Domicilio particular".

La revisión de estas normas no deja dudas en la respuesta a la pregunta central del caso que se comenta: el domicilio es un dato personal confidencial.

La protección de la vida privada mediante el derecho de autodeterminación informativa se vincula especialmente con la protección de datos, es decir, con la información. En este sentido, la discusión que aquí ocupa no se refiere a la protección tradicional del domicilio como espacio físico de residencia de la persona —o sede de la persona jurídica— (Cifuentes 2008, 659-61), sino al domicilio entendido como dato, es decir, al domicilio-dirección. Se trata de dos bienes jurídicamente protegidos distintos y las garantías con que se les rodea también son diversas en naturaleza. Lo mismo pasa con la protección de la imagen de una persona y la protección de las fotografías o registros de esa imagen. También corresponde la diferenciación entre la ideología o creencias religiosas de una persona y los registros de afiliación a un partido o de pertenencia a un credo o iglesia. Otro caso en el que la diferenciación es clara es el de las comunicaciones de la persona, por un lado, y los registros de llamadas o de ubicación de los teléfonos celulares, que son información o datos relacionados con esas comunicaciones.

Cuando el Pacto de San José de Costa Rica hace referencia al domicilio en el artículo 11 —citado por el Tribunal en la sentencia que se

comenta— no se refiere específicamente al domicilio-dirección, sino al domicilio-ámbito de residencia en el esquema tradicional de protección de la vida privada. La aclaración corresponde ya que en los fundamentos de la sentencia pareciera que el Tribunal interpreta este artículo como refiriéndose al domicilio-dirección (SUP-RAP-37/2013, 62).

Conforme a la normativa aplicable al caso, queda claro que el domicilio-dirección es un dato personal confidencial. Una cuestión distinta es dónde y cómo se puede hacer constar y, eventualmente, difundir esa información. Registrar el dato personal en la base de datos de un banco o en el padrón de electores, por ejemplo, es una conducta absolutamente legal y avalada, además, por el consentimiento de la persona que proporciona el dato. Situación distinta es que el banco o la autoridad encargada del padrón electoral ponga esa información en internet, o la entregue o la venda —como sucede en algunos países— a personas o entidades privadas, sin importar qué destino se les den a esos datos.

Los organismos públicos que tienen datos personales en sus registros son garantes de la protección de dichos datos. La LFTAIPG dispone en su artículo 21 que

> Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado consentimiento expreso […], por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

En todos los casos se trata de acciones que facilitan los datos a terceros, no al propio titular de los datos. Este hecho queda claro en el artículo 22, que contempla las hipótesis en las cuales el organismo puede "proporcionar" los datos sin consentimiento del titular. Todas las situaciones contempladas en la excepción se refieren a entregar o facilitar el acceso a los datos a terceros.

En consonancia con dicha obligación, el Reglamento de Transparencia del INE establece, en el artículo 35-1, que

> Los datos personales son información confidencial que no puede otorgarse a una persona distinta que su titular, a menos que exista una autorización expresa de éste. Los servidores públicos del Instituto que intervengan en el tratamiento de datos personales, deberán garantizar la protección en el manejo de dicha información, por lo que no podrá ser comunicada salvo en los casos previstos por la Ley de Transparencia y la Ley.

El artículo 37 del Reglamento refuerza la prohibición de difusión al establecer que

> El Instituto no podrá difundir los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

Las limitaciones mencionadas se refieren precisamente al registro, tratamiento y custodia de la información relativa a los datos personales. Está claro que para difundir, comunicar, proporcionar, distribuir o compartir la información con terceros es necesario el consentimiento expreso del titular de los datos. La necesidad del consentimiento deriva del derecho de autodeterminación informativa de la persona. Cada persona debe saber a quién se entregarán los datos y con qué finalidad, y en función de ello tiene derecho a consentir o no la difusión o entrega de sus datos personales.

El hecho de que una persona haya entregado de forma voluntaria sus datos personales al INE en cumplimiento de los requisitos legales para obtener la credencial para votar no presume su consentimiento para que el Instituto entregue esa información a terceros, salvo en los casos de excepción previstos en la ley.

El artículo 22 de la LFTAIPG establece las hipótesis en las cuales no se requiere el consentimiento del titular: se trata de casos que tienen que ver con intereses superiores al interés personal por la reserva de la vida privada y los datos personales. De acuerdo con la ley mexica-

na, no se requiere el consentimiento del titular cuando los datos son necesarios para fines estadísticos o científicos y se trata de datos disociados —es decir, que no pueden identificarse de manera individualizada con persona alguna—; tampoco se requiere el consentimiento para el cruce de información entre entidades u organismos del Estado para el cumplimiento de sus funciones, ni cuando media una orden judicial para proporcionar los datos personales. Un caso especial previsto en la ley es la posibilidad de proporcionar los datos sin consentimiento del titular en el caso de tercerizar el tratamiento de datos. Es importante señalar que, en este último supuesto, dichos terceros están sujetos a la obligación de confidencialidad y demás criterios de seguridad en el manejo de información y no pueden utilizar los datos con otros fines que no sea la prestación del servicio de tratamiento de datos contratado por el organismo que custodia los datos.

Pero, además de la difusión, distribución y comercialización de datos —conductas que están prohibidas por la ley—, hay otra posibilidad, que es justamente la que describe el caso en análisis: ¿es legal que se haga constar un dato personal en forma visible en un documento (en el sentido amplio del término, por ejemplo, un contrato, un certificado, una escritura, etcétera)? Nadie objetaría que en un contrato figure el domicilio de los contratantes; es más, fijar el domicilio es un requisito de rigor en muchos actos jurídicos. Dichos documentos quedan en control de cada sujeto y cada sujeto es custodio de la reserva de los documentos. Un ejemplo clarísimo: los datos relativos a la salud de una persona son sin duda datos personales protegidos. Cuando se expide un certificado de salud para presentar en la escuela o en el trabajo, ¿se exige que el contenido esté cifrado?, ¿se pide que se exprese por escrito la autorización para que el documento contenga los datos cuya certificación se solicita? A nadie se le ocurre; el dato es reservado y se utiliza el certificado o los resultados de los análisis como se estime conveniente.

Algo similar sucede con el domicilio y otros datos que figuran en el documento de identidad. En algunos países se incluye el nombre del padre y de la madre; en otros se sigue incluyendo el sexo (masculino o femenino), aun cuando se han aprobado leyes de tratamiento igualitario para otras opciones sexuales, y en otros se incluye el esta-

do civil. Si se utilizara el criterio de pedir el consentimiento del titular para la inclusión de cada uno de estos datos personales se podría llegar a reducir el documento de identidad a un plástico con un número o código, y hasta la inclusión de la foto estaría sujeta a consentimiento, por tratarse de datos personales según la LFTAIPG, que los define como "cualquier información concerniente a una persona física identificada o identificable" (artículo 2-II, según texto reformado en 2010).

Por eso es razonable, la respuesta del Ifai a la consulta del IFE fue:

> la inclusión visible de los datos de la calle, número exterior y número interior en la Credencial para Votar no pone en riesgo la protección de los datos personales del ciudadano, "en tanto se genere para el ciudadano información suficiente sobre la importancia de los datos ahí contenidos para que estos adopten ciertas medidas elementales de cuidado y en tanto se propicie una cultura de cuidado responsable para toda persona que en el desarrollo de actividades legitimas posea datos de la credencial para votar".

El principio de confidencialidad en el tratamiento de los datos contenidos en la base de datos —en este caso, el padrón de electores— no resultaría afectado por el hecho de incluir el domicilio completo en forma visible en la credencial para votar.

Las normas mencionadas anteriormente se refieren a la distribución, difusión, comercialización o entrega de datos a terceros, no a la expedición de un documento que se entrega en un único ejemplar y al propio titular de los datos. La seguridad apunta a que no se entregue esa información confidencial a terceros, evitar filtraciones y garantizar que los datos no resulten alterables o se pierdan directamente.

En este sentido, el Tribunal Electoral resolvió un caso interesante relativo a un pedido de acceso a la información pública del padrón de afiliados de un partido. En el expediente SUP-RAP-28/2008 se decidió que se podía entregar la información del nombre y apellido de los afiliados, así como la entidad federativa a la que pertenecían, pero no el dato del domicilio, ya que este es un dato personal confidencial. Con esta solución se respetan tanto el derecho de acceso a la información

pública como el derecho a la protección de los datos personales. Pero, claramente, en este caso se trata del deber de confidencialidad frente a terceros, distinto al de la entrega de la credencial para votar a cada ciudadano con sus propios datos.

La interpretación de las normas debe ser razonable. La visibilidad de un dato personal en un documento o un certificado no implica la difusión, distribución ni comercialización del dato a terceros. Si se equiparara la visibilidad del dato en el documento a las acciones prohibidas por la ley, se llegaría al absurdo de que no se podría entregar al titular de los datos un documento con la información personal que consta en la base de datos salvo en forma encriptada. Sin duda, una interpretación absurda, que significaría, por ejemplo, que los registros civiles no podrían dar partidas de nacimiento o de matrimonio. Entregar estos documentos o certificados es precisamente una de las funciones propias de los registros públicos.

Tanto la LFTAIPG como las demás normas reglamentarias y los lineamientos reseñados se refieren al registro, custodia y tratamiento de datos cuando establecen la obligación de confidencialidad, y es discutible que entregarle a una persona un documento oficial en el que aparece su propio domicilio signifique violar la regla de confidencialidad. Entregar el documento al titular de los datos no implica difundir, distribuir ni comercializar el dato personal a terceros, que es lo que está prohibido sin consentimiento del titular. En esta línea, el Reglamento del INE es claro cuando dispone que "los datos personales son información confidencial que no puede otorgarse a persona distinta de su titular, a menos que exista una autorización expresa de éste" (artículo 35). Incluir el dato del domicilio en forma visible no implica violar esta regla. Es el titular de la credencial quien se transforma en custodio de la confidencialidad de los datos que constan en el documento.

El domicilio, entendido como dirección (*address*), no es considerado un dato personal sensible que requiere confidencialidad en todos los países. En muchos casos el domicilio-dirección se considera un dato "libre", generalmente accesible y usable, al igual que el nombre, el apellido, la fecha de nacimiento o el número de identificación

personal.[7] El tratamiento del dato de domicilio en los documentos de identidad no es unánime en los países latinoamericanos. Se utiliza el ejemplo del documento de identidad porque no todos los países cuentan con una credencial especial para votar, pero todos tienen un documento de identidad. El domicilio completo no figura en el documento de identidad en 12 países: Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Panamá, Paraguay, Uruguay y Venezuela. En seis países sí aparece en el anverso o reverso del documento: Argentina, Bolivia, Cuba, Nicaragua, Perú y República Dominicana.[8]

IV. Valoración de la solución adoptada

Tanto la decisión del Tribunal en el caso SUP-RAP-37/2013 como el acuerdo CG292/2013 del IFE —dictado como consecuencia de la sentencia— adoptan una solución razonable y plenamente ajustada al principio de legalidad, en tanto dejan en manos de cada persona la decisión acerca de la forma en que el domicilio aparecerá en su credencial para votar. Sin perjuicio de lo cual también había razones para sostener la validez y legalidad de la primera decisión del IFE en cuanto a la inclusión visible del domicilio en la credencial para votar.

En síntesis, la solución adoptada se ajusta al ordenamiento jurídico mexicano y a los principios generales aplicables a la protección de los datos personales. Los ejes de la solución se refieren a los siguientes puntos:

1) El domicilio debe figurar en la credencial para votar. El Código Federal de Instituciones y Procesos Electorales establece expresamente que el domicilio es uno de los datos que debe contener la credencial para votar, aunque no establece nada respecto a la forma en que la información debe estar contenida. La determinación del formato a adoptar es una facultad del INE.

---

7 Véanse Simitis (1983, 171-77) y Gregorio [(2007), en especial el punto 3 acerca de acceso a registros públicos mediante internet)].

8 La información fue chequeada con colegas de cada uno de los países entre el 23 y 24 de noviembre de 2014.

2) La función de la credencial para votar es identificar al elector y habilitar el sufragio. Ambas funciones pueden cumplirse en plenitud sin necesidad de que el domicilio figure en forma visible. La no visibilidad del domicilio en la credencial para votar no afecta los acuerdos que permiten su utilización como documento de identidad hasta que se implemente la cédula de identidad, ello es así ya que la Ley de Población no incluye el domicilio entre los datos contenidos en la cédula.
3) El domicilio es un dato personal y confidencial. Tanto la Constitución como las leyes referidas al acceso a la información pública gubernamental y a la que está en manos de los particulares reconocen la protección de los datos personales entendidos de forma amplia como cualquier información referida a una persona identificada o identificable. Las normas del IFE acerca de transparencia y protección de datos expresamente reconocen que el domicilio es un dato personal y disponen la confidencialidad de dicha información salvo consentimiento expreso y documentado del titular del dato.
4) El derecho de autodeterminación informativa justifica la consulta a cada persona. La Constitución y la legislación mexicanas garantizan el derecho a la autodeterminación informativa como una manifestación más de la protección a la vida privada. La resolución de dejar en manos de cada ciudadano la decisión sobre si desea que su domicilio figure en forma visible en la credencial para votar es congruente con este derecho. El domicilio figurará siempre en forma cifrada en el documento ya que es uno de los contenidos exigidos en la ley.

Con esta solución se conjugan de manera armónica el interés general por la transparencia, certeza y confiabilidad del proceso electoral, y el derecho de cada persona a la protección de su intimidad y el control de la información relativa a sus datos personales.

Fuentes consultadas

Alvarez-Cienfuegos Suárez, José María. 1999. *La defensa de la intimidad de los ciudadanos y la tecnología informática*. Pamplona: Aranzadi.

Bustillos Roqueñí, Jorge. 2011. La protección de los datos personales en materia político-electoral. En *Retos de la protección de datos personales en el sector público*. México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Cifuentes, Santos. 2008. *Derechos personalísimos.* 3.ª ed. Buenos Aires: Astrea.

Corte de Justicia de la Unión Europea. Sentencia del 13 de mayo de 2014 en el caso C 131/2012, "Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González". Disponible en http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=es&type=TXT&ancre= (consultada el 15 de mayo de 2014).

Crónica. Disponible en http://www.cronica.com.mx/notas/2014/835427.html (consultada el 20 de noviembre de 2014).

Directiva 95/46/CE del Parlamento Europeo. 1995. Disponible en http://www.wipo.int/wipolex/es/details.jsp?id=13580.

Ferreira Rubio, Delia. 1982. *El derecho a la intimidad. Análisis del art. 1071 bis del Código Civil.* Buenos Aires: Editorial Universidad.

——. 1999. Comentario al artículo 1071 bis del Código Civil. El derecho a la intimidad. En *Código Civil y normas complementarias. Análisis doctrinal y jurisprudencial*, eds. Alberto J. Bueres y Elena I. Highton. Buenos Aires: Hammurabi.

Gregorio, Carlos G. 2007. Protección de datos personales en América Latina-Juan Pérez ante una disyuntiva de progreso y bienestar. En *Informe Situacional de Privacidad y Acceso a la Información en América Latina.* Lima: UNESCO-Alfa Redi. [Disponible en http://www.iijlac.org/docs/juanperez.pdf].

Guerra Ford, Oscar M. 2011. Las legislaciones de protección de datos personales en el país. En *Retos de la protección de datos personales en el sector público.* México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Hassemer, Winfried y Alfredo Chirino Sánchez. 1997. *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos.* Trad. Alfredo Chirino Sánchez. Buenos Aires: Editores del Puerto.

IFE. Instituto Federal Electoral. Acuerdo CG732/2012. Disponible en http://www.ine.mx/docs/IFE-v2/DS/DS-CG/DS-SesionesCG/CG-acuerdos/2012/Noviembre/CGext201211-21/CGe211112ap3.pdf (consultada el 15 de octubre de 2014).

——. Acuerdo CG733/2012. Disponible en http://www.ine.mx/docs/IFE-v2/DS/DS-CG/DS-SesionesCG/CG-acuerdos/2012/Noviembre/CGext201211-21/CGe211112ap4.pdf (consultada el 15 de octubre de 2014).

——. Acuerdo CG84/2013. Disponible en http://www.ine.mx/docs/IFE-v2/DS/DS-CG/DS-SesionesCG/CG-acuerdos/2013/Febrero/CGext201302-27/CGe270213ap8.pdf (consultada el 20 de noviembre de 2014).

——. Acuerdo CG292/2013. Disponible en http://www.ine.mx/docs/IFE-v2/DS/DS-CG/DS-SesionesCG/CG-acuerdos/2013/Octubre/CGext201310-23/CGex201310-23ap6.pdf (consultada el 20 de noviembre de 2014).

INE/CG70/2014. Reglamento del Instituto Nacional Electoral en materia de Transparencia y Acceso a la Información Pública. Disponible en http://norma.IFE.org.mx/documents/27912/276852/2014_Regto_Transparencia.pdf/8dffabb3-fed9-421a-80f9-2b9ebff9d879 (consultada el 18 de agosto de 2014).

Jóri, András. 2007. *Data Protection Law - An Introduction.* Disponible en http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy (consultada el 18 de agosto de 2014).

Lavalle Cobo, Dolores. 2009. *Derecho de acceso a la información pública*. Buenos Aires: Astrea.

LFTAIPG. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Disponible en http://www.normateca.gob.mx/Archivos/66_D_3887_29-07-2014.pdf (consultada el 30 de noviembre de 2014).

Lineamientos Generales para la Clasificación y Desclasificación de la Información del IFE. Disponible en http://norma.IFE.org.mx/documents/27912/286859/2011_Lineamientos_Clas_Descla_IFE.pdf/84a118fb-b8f3-44e4-bea0-67ddc4b22be8 (consultada el 24 de noviembre de 2014).

ONU. Organización de las Naciones Unidas. 2014. Disponible en http://www.zdnet.com/un-moves-to-strengthen-digital-privacy-7000036163/ (consultada el 28 de noviembre de 2014).

Remolina Angarita, Nelson. 2014. Latinoamérica y protección de datos personales en cifras (1985-2014). Disponible en http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/2014-Latinoamerica-proteccion-datos-en-cifras-1985-2014-Remolina.pdf.

Rodotá, Stefano. 1983. Data Protection. Some Problems for Newcomers. En *Legislation and Data Protection.* Roma: Council of Europe-Camera dei Deputati.

Sentencia SUP-RAP-28/2008. Disponible en http://portal.te.gob.mx/colecciones/sentencias/html/SUP/2008/RAP/SUP-RAP-00028-2008.htm (consultada el 10 de octubre de 2014).

—— SUP-RAP-37/2013. Actor: Partido Acción Nacional. Autoridad responsable: Consejo General del Instituto Federal Electoral. Disponible en http://portal.te.gob.mx/colecciones/sentencias/html/SUP/2013/RAP/SUP-RAP-00037-2013.htm (consultada el 15 de noviembre de 2014).

—— SUP-RAP-182/2013. Recurrentes: Partidos de la Revolución Democrática y del Trabajo. Autoridad responsable: Consejo General del Instituto Federal Electoral. Disponible en http://portal.te.gob.mx/colecciones/sentencias/html/SUP/2013/RAP/SUP-RAP-00182-2013.htm (consultada el 21 de noviembre de 2014).

Shattuck, John H. F. 1977. *Rights of Privacy.* Skokie: National Textbook Co.

Simitis, S. 1983. Data protection. A few critical remarks. En *Legislation and Data Protection.* Roma: Council of Europe-Camera dei Deputati.

Zamudio Salinas, Ma. de Lourdes. 2012. "El marco normativo latinoamericano y la ley de protección de datos personales del Perú". *Revista Internacional de Protección de Datos Personales* 1 (julio-diciembre).