Ciudad Autónoma de Buenos Aires, 2 de noviembre de 2016

VISTO:

El trámite nº **15553/16**, iniciado de oficio por esta Defensoría del Pueblo, a fin de analizar la cesión y tratamiento de los datos personales de los/as vecinos/as de la Ciudad Autónoma de Buenos Aires, en el marco de la firma de los convenios de cooperación entre la Administración Nacional de la Seguridad Social (A.N.Se.S.) y el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP) con la Secretaría de Comunicación Pública dependiente de la Jefatura de Gabinete de Ministros de la Nación.

Y CONSIDERANDO QUE:

I.- Hechos

Mediante Resolución nº 166-E/2016 (publicada en el Boletín Oficial de fecha 25 de julio de 2016), la Jefatura de Gabinete de Ministros de la Nación aprobó la firma del Convenio Marco de Cooperación entre la Secretaría de Comunicación Pública de la Jefatura de Gabinete de Ministros de la Nación y la A.N.Se.S. (fs. 7/10).

Asimismo, por Resolución nº 1005/16 (publicada en el Boletín del Instituto Año XII nº 2565 de fecha 14 de junio de 2016), el Director Ejecutivo del INSSJP aprobó un acuerdo similar; en el caso se trata de un modelo de convenio marco -al inicio de la presente no había sido suscripto- entre ese organismo y la citada Secretaría de Comunicación Pública, que también fue objeto de estudio en el presente trámite (fs. 27/30).

En ambas situaciones, se conviene la cesión electrónica periódica de las bases de datos de la A.N.Se.S. en relación a las siguientes referencias personales:

a) Nombre/s y Apellido/s;
b) Documento Nacional de Identidad (D.N.I.);
c) Clave Única de Identificación Tributaria (C.U.I.T.) / Clave Única de Identificación Laboral (C.U.I.L.);
d) Domicilio;
e) Teléfono/s;
f) Correo Electrónico;

g) Fecha de Nacimiento;
h) Estado Civil;
i) Estudios.

El objeto central consiste en *"...establecer un marco técnico y jurídico para el intercambio electrónico de información entre LAS PARTES, contenida en sus bases de datos consolidadas (…) acordando que dicha información será utilizada a fin de mantener informada a la población, así como para identificar y analizar las problemáticas o temáticas de interés en cada localidad del país que permita incorporar la diversidad federal en la comunicación pública..."* (fs. 13).

Respecto al uso que hará la Secretaría de Comunicación Pública, se señala la necesidad de mantener informada a la población *"…a través de diversas modalidades, que incluyen desde las redes sociales y otros medios de comunicación electrónicos, hasta el llamado telefónico o la conversación persona a persona, de forma de lograr con los ciudadanos un contacto individual e instantáneo..."*, y que además con análoga finalidad *"...resulta necesario contar con herramientas que permitan instrumentar las políticas de comunicación (…) destacándose la posibilidad de enriquecerlas, segmentarlas, clasificarlas y normalizarlas, para posteriormente compartirlas con el organismo dador..."* (fs. 8).

La Dirección Nacional de Protección de Datos Personales dependiente del Ministerio de Justicia y Derechos Humanos de la Nación, preopinó en ambos casos. En sendos dictámenes aplicó la Ley Nacional nº 25.326 de Protección de Datos Personales. En un caso lo realizó por Nota DNPDP nº 980/16 (fs. 21/26) y en el otro mediante Dictamen DNPDP nº 5/16 (fs. 2/6).

En el presente trámite se agregaron los actos administrativos aprobatorios del Convenio firmado con la A.N.Se.S. y el del modelo de Convenio a suscribirse con el INSSPJ. A fs. 11/18, figura el firmado en el primer caso y el modelo que se firmaría en el segundo obra a fs. 27/30.

Se agregó normativa específica como la Resolución nº 952/2008 de la A.N.Se.S., que aprueba las políticas de intercambio electrónico de información (fs. 39/43).

Asimismo, se glosaron notas periodísticas que dan cuenta de la repercusión de la cuestión (fs. 31/33).

Se remitieron oficios dirigidos a la A.N.Se.S. (fs. 19); a la Secretaría de Comunicación Pública (fs. 20) y al INSSJP (fs. 34/35).

A fs. 36/38, se anexó la respuesta de la Secretaría de Comunicación Pública, que en su parte sustancial destaca que la Dirección Nacional ha realizado un análisis pormenorizado del caso en el que se concluyó que *"…'no se observa impedimento legal para la suscripción del Convenio Marco previsto'..."*. Asimismo, se señaló que *"…las medidas de protección de los datos cedidos no serán de diferente idoneidad de aquellas con que los resguarda el cedente, estableciéndose mecanismos de seguridad informática que permitan el exclusivo uso por parte del Estado Nacional, cumpliendo los principios de finalidad y pertinencia, es decir, los mismos serán utilizados a efectos de mantener informada a la población, sobre aquellos temas de interés público..."*.

Luego, se agregó que *"...En lo atinente al artículo 4.3 de la ley citada, y en consonancia con lo acordado en la cláusula primera del presente convenio, que constituye su objeto, es dable mencionar que el mismo no luce incompatible con aquel que originó la obtención de datos por parte de la ANSES. Y por otra parte la transferencia se encuentra expresamente avalada en el artículo 11 inciso 3, apartado c. de la mencionada ley. (…) En cuanto al análisis sobre la proporcionalidad y pertinencia, los mismos se encuentran insertos en su totalidad en el Expediente por el cual tramitó el Convenio de maras, y especialmente en el Dictamen del Servicios Jurídico Permanente. Sin embargo, a efectos de ponerlo en su conocimiento, los datos objeto de cesión son en su mayoría absolutamente públicos, ninguno de ellos revista la calidad de 'datos sensibles' de acuerdo a la ley 25.326; se trata en realidad de información mínima para mantener informada a la población sobre cuestiones de su interés cotidiano, es decir son proporcionados, porque son los datos mínimos necesarios con que debemos contar para que el objetivo comunicacional se alcance. Y resultan por cierto pertinentes, porque se trata de mensajes de interés público, como campañas de prevención en materia de salubridad o de seguridad; o la difusión de beneficios, facilidades, subsidios, etc.; todos respecto de los cuales el conocimiento del ciudadano sobre su existencia y características resulta sustancial..."*.

Por su parte el INSSJP respondió con cierto retraso sin agregar elementos relevantes para el análisis del caso. La respuesta, obrante a fs. 74/75, reiteró que el Acuerdo en estudio fue analizado por la Dirección Nacional de Protección de Datos Personales y que existía compatibilidad entre los datos de su Organismo y la Secretaría de Comunicación Pública. En concreto refirieron que *"...cabe señalar que las obligaciones asumidas por las partes se encuentran en línea con lo dispuesto en la Ley Nº 25.326 de protección de datos personales, conforme surge del referido dictamen de la Dirección Nacional de Protección de Datos Personales. En efecto, consta en el convenio que la información a transferir en virtud del mismo no se trata de datos calificados como 'sensibles' (art. 2*

Ley 25.326). Asimismo, es de destacar que las partes se comprometen a adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos (cfr. artículos 9 y 10 Ley 25.326). Del convenio también surge que existe una compatibilidad entre la finalidad para la cual el Instituto obtuvo la información de sus usuarios y la finalidad para la cual será utilizada por parte de la Secretaría de Comunicación, conforme lo exigido por el artículo 4º, inc. 3º de la Ley 25.326...".

La A.N.Se.S., a través de la Dirección General Diseño de Normas y Procesos, hizo saber en su respuesta que *"...esta Dirección entiende que el Convenio Marco de Cooperación que integra como anexo la Resolución E/2016 de la Jefatura de Gabinete de Ministros de fecha 21 de julio de 2016, cumple con la normativa vigente en materia de Protección de Datos Personales y con la Resolución DE Nº 952/08, en la cual se aprueba la Política de Intercambio Electrónico de Información del Organismo. En el mismo sentido, se señala que en las cláusulas PRIMERA, SÉPTIMA, OCTAVA, NOVENA, DÉCIMA PRIMERA, DÉCIMA SEGUNDA, DÉCIMA TERCERA, DÉCIMA CUARTA, DÉCIMA QUINTA Y DÉCIMA OCTAVA del referido Convenio se enumeran expresamente las pautas referidas al uso, la manipulación y las medidas de seguridad que deben adoptar las partes en virtud del acuerdo suscripto..."* (fs. 59).

II.- <u>Competencia de la Defensoría del Pueblo</u> (Centro de Protección de Datos Personales)

El art. 22 de la Ley nº 1.845 publicada en el año 2007 dispone lo siguiente *"Organismo de control - Desígnase a la Defensoría del Pueblo de la Ciudad de Buenos Aires como organismo de control de la presente ley"*.

A su turno el art. 23 establece que este Órgano Constitucional debe *"...Velar por el cumplimiento de las disposiciones de la presente ley y por el respeto de los derechos al honor, la autodeterminación informativa y la intimidad de las personas. Formular advertencias, recomendaciones, recordatorios y propuestas a los responsables, usuarios y encargados de archivos, registros, bases o bancos de datos del sector público de la Ciudad de Buenos Aires, a los efectos de lograr una completa adecuación y cumplimiento de los principios contenidos en la presente ley (…) Colaborar con la Dirección Nacional de Protección de Datos Personales y con los correspondientes organismos de control provinciales en cuantas acciones y actividades sean necesarias para aumentar el nivel de protección de los datos personales en el sector público de la Ciudad de Buenos Aires..."*.

En el supuesto en estudio, se dan tales extremos

toda vez que la información contenida en la A.N.Se.S. y en el INSSJP comprende datos personales de habitantes de esta Ciudad.

Es por ello que en virtud de lo dispuesto por la Ley nº 1.845 y por imperio de la Ley nº 3 y el art. 137 de la Constitución de la Ciudad Autónoma de Buenos Aires, corresponde tomar intervención en el caso toda vez que *"Es misión de la Defensoría la defensa, protección y promoción de los derechos humanos y demás derechos y garantías e intereses individuales, colectivos y difusos tutelados en la Constitución Nacional, la Constitución de la Ciudad y las leyes, frente a los actos, hechos u omisiones de la administración, de prestadores de servicios públicos..."*.

Además dicha información es captada de bases de datos locales que recaban antecedentes laborales, sobre aportes y servicios, discapacidad, entre mucha otra contenida y generada por la Ciudad. Esto es así dado que la A.N.Se.S. es el órgano nacional encargado de *"...administrar y controlar la recaudación de los fondos correspondientes a los regímenes nacionales de jubilaciones y pensiones, en relación de dependencia y autónomos, de subsidios y asignaciones familiares y al Fondo Nacional de Empleo, así como la fiscalización del cumplimiento de las obligaciones de aquéllos."* (art. 2º del Decreto nº 2741/91).

En efecto la cesión y tratamiento de la información personal existente en las bases manejadas por la A.N.Se.S. y el INSSJP constituyen un dato personal en los términos de la Ley Nacional nº 25.326 (art. 11) y la Ley nº 1.845 (arts. 26/28 y 38) de esta Ciudad. Dicha cuestión es además reconocida por el mismo Estado Nacional en la cláusula octava del Convenio suscripto entre la A.N.Se.S., el INSSJP y la Secretaría de Comunicación Pública en el que se apela expresamente a la Ley nº 1.845.

Por las razones expuestas, este Organismo posee competencia indubitable para buscar la protección de los derechos de las personas.

III.- Reseña histórica del surgimiento del derecho a la protección de datos personales

Dada la naturaleza de la cuestión que se aborda, no resulta ocioso realizar una breve historia de la protección de datos personales y el rol del Estado en la materia. Cabe destacar que todas las referencias se ubican en la década de los setenta del siglo pasado.

El primer caso, cronológicamente analizado, es el que se produjo en el Land de Hesse (uno de los Estados Federados de

Alemania) en el año 1970, mediante el cual se aseguró la protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal. A efectos de asegurar el cumplimiento de sus previsiones, se creó por Ley Comisario de Protección de Datos, al cual se le garantizaba independencia para el desempeño de sus funciones, que eran velar por la observancia de los preceptos de la propia ley y a cuantas otras hicieran referencia al trato de los datos de los ciudadanos.

Dos años después, en 1972, estalló en los Estados Unidos de Norteamérica, el escándalo conocido por el nombre de Watergate, en el cual sustrajeron cintas de grabación del Comité de Campaña del Partido Demócrata por encargo del entonces Presidente Richard Nixon.

Las consecuencias de ese episodio fueron dos: por un lado la renuncia del Presidente en el mes de agosto de 1974 y, por el otro, la sanción -el día 31 de diciembre de ese año- de la Privacy Act. La exposición de motivos de la Privacy Act de 1974, manifestó que su objetivo era proteger la privacidad de los individuos identificados en sistemas de información llevados por entes y órganos federales mediante la regulación de la captación, conservación, uso y difusión de información por éstos, y que se prescindía del soporte que la contenía, de modo que la ley resultaba aplicable ya sea que las operaciones de tratamiento se realizaran por medios informáticos o manuales.

En el año 1976 se sancionó la nueva Constitución de Portugal. En dos artículos del texto fundamental (26 y 35) aparecen la intimidad y privacidad concatenadas con la noción de protección de datos personales. En el primero de ellos se reconoce a todos los ciudadanos el derecho a la identidad personal, al desarrollo de la personalidad, a la capacidad civil, a la ciudadanía, al buen nombre y reputación, a la imagen, a la palabra, a la reserva de la intimidad de la vida privada y familiar y a la protección legal contra cualesquiera formas de discriminación y determina que la ley establecerá garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana, de informaciones relativas a las personas y a las familias. Por su parte el art. 35, en su inc. 2, establece que la ley será la que defina -de manera minuciosa- el concepto de datos personales, y las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección por medio de un órgano administrativo independiente.

Tan sólo dos años después, en 1978, fue el Reino de España que, tras la restauración de la democracia, sancionó un nuevo

texto constitucional, que en su art. 18 dice *"Derecho a la intimidad. Inviolabilidad del domicilio: Artículo 18 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

Como puede derivarse de lo expuesto *ut supra,* en todos los casos citados, la normativa garantiza el manejo adecuado, ponderado y respetuoso de los derechos de la ciudadanía por parte del Estado. Este atributo adquiere especial relevancia en los casos de Portugal y España, toda vez que el carácter constitucional asignado en ambos países, es uno de los pilares de la recuperación de las garantías individuales y los derechos políticos y sociales de la ciudadanía luego de que resultaran abolidos por más de 40 años por los regímenes autoritarios de Antonio de Oliveira Salazar y Francisco Franco.

Aparte de una contextualización de la protección de datos personales por parte del Estado producida en el último cuarto del siglo anterior, adquiere especial relevancia en el caso que nos ocupa que tanto la figura constitucional como la legislación nacional al respecto abrevan en la experiencia española. Igual consideración debemos formular en relación a la normativa local (Ley nº 1.845) que como se dijera le otorga competencias a este Órgano Constitucional.

IV.- <u>Recolección de información personal por parte del Estado</u>

El Estado como persona jurídica, puede recolectar información de los ciudadanos. Sin embargo, esta prerrogativa no es ilimitada, debe hacerse por razones justificadas y en el marco del cumplimiento de ciertos principios, entre ellos, el respecto de los derechos individuales. En esta línea la normativa en materia de habeas data consagra el principio de calidad del dato que hace que los recolectados sean pertinentes, adecuados, no excesivos y utilizados en el marco del fin de su recolección. Asimismo, dicha normativa parte del supuesto de que la titularidad de la información personal corresponde a cada uno de los sujetos y que el Estado los posee en calidad de depositario de los mismos, por ende para hacer tratamiento de estos debe solicitar autorización a su titular.

La Asamblea General de las Naciones Unidas en el año 2014 en su declaración sobre el derecho a la privacidad en la era digital

ha exhortado a *"...todos los Estados a que: a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales; b) Adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos; c) Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos; d) Establezcan o mantengan mecanismos nacionales de supervisión, de índole judicial, administrativa o parlamentaria, que cuenten con los recursos necesarios y sean independientes, efectivos e imparciales, así como capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado; e) Proporcionen acceso a un recurso efectivo a las personas cuyo derecho a la privacidad haya sido violado mediante la vigilancia ilícita o arbitraria, de conformidad con las obligaciones internacionales en materia de derechos humanos; 5. Alienta al Consejo de Derechos Humanos a que siga ocupándose activamente del debate con el fin de determinar y aclarar los principios, normas y mejores prácticas relativos a la promoción y protección del derecho a la privacidad y a que considere la posibilidad de crear un procedimiento especial con ese fin; 6. Decide seguir ocupándose de la cuestión..."*[1].

En nuestro País, con motivo del fallo Halabi[2], la doctrina ha subrayado que *"En diversos países del mundo vemos cómo late la idea de limitar de forma cierta el poder de las comunicaciones, básicamente debido a la irregularidad del uso de la información para fines distintos de aquellos reconocidos legalmente en perjuicio de las personas. Las comunicaciones en general y la informática en particular representan una fuente indiscutible de progreso económico, social y cultural, ello no obstante poseer ciertas cualidades que se deben analizar a la luz de la protección de los derechos individuales. Por ello hay que tener en cuenta que no sólo los datos sensibles pueden provocar conflictos al ser utilizados,* ***sino también que datos que no entran dentro de esta categoría, al ser conectados con otros, pueden dar determinados perfiles de la persona, lo que atentaría del mismo modo contra su intimidad****. En las legislaciones de muchos países encontramos normas que protegen la intimidad de las personas, así como los datos que se guardan sobre ellas..."*[3] (lo resaltado es propio).

1 Resolución aprobada por la Asamblea General de las Naciones Unidas del 18 de diciembre de 2014 -69/166- sobre el derecho a la privacidad en la era digital.
2 "Halabi Ernesto c/PEN Ley 25.873 dto. 1563/04 s/Amparo Ley 16.986" Expediente 5657/05.
3 Halabi, Ernesto *"El derecho a la Intimidad y la Ley Espía"*, UtSupra.com, 2009, pág. 93.

También se ha señalado que *"…de todas formas cuestionamos que no se haya respetado el deber de información que debe acompañar a esa sesión: consideramos que ese deber -que surge del artículo 11 de la ley 25.326- es independiente de la obtención previa del consentimiento. Ese deber de información permite que los ciudadanos conozcan quien almacena y da tratamiento a sus datos personales, lo que les permite mantener cierto grado de control sobre los mismos y vigilar que no se haga un mal uso de ellos"*[4]. Por ello, en el caso concreto, nada impedía que se haga una consulta a los ciudadanos para luego proceder al tratamiento de sus datos personales aspecto que sería independiente de la necesidad del consentimiento previo.

En esta línea, el Reglamento Europeo en materia de protección de datos personales dispone que *"...El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta"* (Cons. 32). Y también, en el inc. 11 del art. 4º, relativo a las definiciones, establece lo siguiente *"...consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen..."*; en el inc. 3 del art. 7º se señala que *"...El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo..."*[5].

En resumen, el Estado debe ser uno de los

4 *"El Estado Recolector"*, setiembre de 2014, https://adcdigital.org.ar/wp-content/uploads/2016/01/El-Estado-recolector.pdf, realizado por la Asociación por los Derechos Civiles (ADC).

5 Reglamento (UE) 2016/679 Diario Oficial de la Unión Europea http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

principales garantes de la protección a la privacidad.

V.- Principios en materia de protección de protección de datos personales

Existen diversos principios en materia de protección de datos personales que son aplicables al caso en estudio. En el Titulo III de la norma, se fija un cuerpo robusto en pos de los derechos de los individuos. Así entre los arts. 6º a 12, se regula y garantiza el modo en que deben recogerse los datos personales, aspectos sobre el consentimiento del titular, protección para los datos sensibles y la cesión y/o transferencia.

También, rige el principio de autodeterminación informativa. El mismo, está contemplado en el art. 1º de la Ley nº 1.845 y es el que permite que los individuos tengan el control respecto de qué se hace con sus datos. Este *"…exigiría que todo tratamiento de datos estuviere autorizado por los afectados; esto es, si el afectado no diere su consentimiento, nadie podría tratar su datos..."*[6].

Asimismo, el principio de calidad del dato apunta a que la información obtenida sea cierta, adecuada, pertinente y no excesiva en relación al ámbito y finalidad para los que se hubieren obtenido. La doctrina lo ha explicado como el uso razonable de la información de los otros *"...en virtud de lo cual sólo podría ser objeto de tratamiento aquellos datos que resultasen adecuados para la finalidad recogida), congruencia (los datos no podrían ser utilizados para una finalidad distinta de la de recogida..."*[7].

Por su parte, el principio de finalidad del dato es central en el caso en estudio *"La aplicación de los datos a la finalidad para la que fueron recabados constituye un principio fundamental en materia de protección de datos y cada vez despliega mayor relevancia. La conexión entre recogida-tratamiento de datos y finalidad es un elemento fundamental del derecho de protección de datos"*[8]. Esto demuestra que cuando la información de cada uno de los individuos es utilizada con fines distintos de aquellos que motivaron su recolección, estamos frente a un uso incompatible y contrario a la normativa.

---

6 Poullet Yves, María Verónica Pérez Asinari, Palazzi Pablo (coordinadores) *Derecho a la Intimidad y a la Protección de Datos Personales*, Heliasta, 2009, pág. 106.

7 Poullet Yves, María Verónica Pérez Asinari, Palazzi Pablo (coordinadores) *Derecho a la Intimidad y a la Protección de Datos Personales*, Heliasta, 2009, pág. 106.

8 Lemes Serrano, Carlos, Buisan García Nieves, *La Ley de Protección de Datos: análisis y comentario de su jurisprudencia* , Editorial Lex Nova, 2008, página 146 Disponible en https://books.google.com.ar/books?id=0-P07_iKg_UC&pg=PA19&dq=principio+de+finalidad+del+dato+definici%C3%B3n&hl=es&sa=X&ved=0ahUKEwjyqd7qgcbOAhXITZAKHVHQCX0Q6AEIITAB#v=snippet&q=principio%20de%20finalidad&f=false

VI.- Legislación en materia de protección de datos personales

Dicho lo previo, vale remarcar los principales aspectos que contempla el cuerpo normativo en materia de protección de datos personales. No es ocioso destacar que se sienta en la razón fundamental que tiente todo ser humano a la dignidad y a la protección de sus acciones privadas. Así, el art. 19 de la Constitución Nacional reza *"Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios y exentas de la autoridad de los magistrados..."*. En igual dirección lo hace el art. 12 de la Constitución local.

Sobre esa base, tanto la Constitución Nacional -en el art. 43- como la Constitución local -en el art. 16- prevén la figura de habeas data. Esta garantía se encuentra en línea con la protección del derecho al honor y la intimidad de las personas que debe estar libre toda injerencia arbitraria tal como lo garantizan por los tratados internacionales de derechos humanos aplicables a nuestro sistema[9].

En el ámbito nacional la Ley nº 25.326, fija pautas concordantes que son expuestas en el Dictamen y Nota respectivamente de la Dirección Nacional de Protección de Datos Personales (fs. 2/6 y 21/26). Por un lado, en inc. 1 y 3 del art. 4º contienen el concepto de *"finalidad del dato"*. Además, el art. 5º referido al consentimiento, establece que *"...1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias (…) 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio..."*.

Por su parte el art. 11, referido a cesión señala que *"...1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. 2. El consentimiento para la cesión es revocable. 3. El consentimiento no es exigido cuando: a) Así lo disponga una ley; b) En los supuestos previstos en el artículo 5º inciso 2; c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas*

9 Constitución Nacional: inc. 22 del art. 75; y en la Constitución de la Ciudad Autónoma de Buenos Aires: art. 10.

competencias; d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables. 4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".

La Ley nº 1.845 en el Titulo III, contiene de manera generosa los principios vigentes en la materia. En primer término, consagra el principio de calidad de los datos (art. 6º); y luego se completa el blindaje con el requisito en relación a que la recolección y señala que *"...no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas con aquéllas que motivaron su obtención..."*. Asimismo, se solicita que el titular del dato preste su consentimiento escrito para el tratamiento de la propia información salvo que *"...Los datos personales se recaben para el ejercicio de funciones propias de los poderes de la Ciudad de Buenos Aires, o en virtud de una obligación legal (…) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio..."* (inc. 4 del art. 7º) (lo subrayado es propio).

El art. 10 del Título III de la citada norma, destaca que *"...Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo"* (lo subrayado es propio).

De la simple lectura de la norma, el consentimiento del titular del dato, es un principio madre en materia de habeas data, por tanto sus excepciones deben ser aplicadas cuidadosamente. Efectivamente, dado que el traspaso de los datos personales consiste en entregar información personal, en principio se requiere el consentimiento del titular del dato, éste es un requisito que hace a la licitud de su tratamiento.

Por ende, de los hechos se advierte que no se ha pedido autorización al titular de los datos y tampoco existe un interés legítimo entre el cedente y el cesionario.

VII.- Análisis del caso

Del análisis efectuado se desprende que no existe en la cesión de información por parte de los órganos cedentes un interés concordante, análogo o relacionado con el cesionario. Es decir, que no hay compatibilidad entre el fin que persigue la información recogida y tratada por la A.N.Se.S. y el INSSJP, y la aplicación que de ella haría la Secretaría de Comunicación Pública, en razón de lo cual no se cumple con los requisitos de los arts. 6º, 7º y con el inc. 1 del art. 10 de la Ley nº 1.845.

Por ello, y a fin de parafrasear a la Dirección Nacional de Protección de Datos Personales (DNPDP) en otro caso: *"Lo expuesto implica que será requisito sustancial para la licitud de la cesión que la misma tenga sustento en las competencias otorgadas al organismo respecto de la información a ceder. Por tales motivos, cabe concluir que la cesión pretendida no resultará legítima, por no reunir los requisitos previstos en los arts. 5º y 11 de la Ley Nº 25.326 relativos a la competencia del Organismo y el interés legítimo del cesionario"*[10].

En este punto cabe mencionar que la Secretaría de Comunicación, tiene como responsabilidad primaria *"Asistir en el desarrollo, planificación y ejecución de la comunicación y difusión de los actos del Sector Público Nacional hacia la comunidad en su conjunto. Efectuar el control operativo de las acciones de comunicación pública, en el ámbito de su competencia"*[11]. Por su parte, la A.N.Se.S., es un organismo descentralizado que tiene entre sus funciones el otorgamiento y pago de las jubilaciones y pensiones, el pago de asignaciones familiares, la gestión y liquidación por desempleo, el pago de la Asignación Universal por Hijo para Protección Social, entre otras. Por su parte el INSSJP, tiene por principal misión brindar el *"Plan de Asistencia Médica Integral–, con el fin de brindar atención médica, social y asistencial a una población específica: los adultos mayores"*[12].

En efecto, el estudio de compatibilidad requerido para este tipo de cesiones, no aparece justificado toda vez que las responsabilidades primarias de los organismos difieren sustancialmente, además de que como ya se señaló, el uso que se haría de los datos que surge de los Convenios y no se encuentra acorde con la finalidad por la que estos fueron recabados. De modo tal que no es viable la remisión de la totalidad de la información contenida en las diversas bases de datos con el fin de mantener mejor informada a la población cosa que, eventualmente, podría

10 Dictamen REF: EXP Nº 1-2015-1695285/2015 DICTAMEN DNPDP Nº 19/15 http://www.jus.gob.ar/media/3146373/d2015_19.pdf

11 Información obtenida de: http://mapadelestado.modernizacion.gob.ar/sitio/jgm/jgm_resp_prim_y_acc_scp.html

12 Información obtenida http://www.pami.org.ar/me_in_historia.php

hacerse con el previo consentimiento del titular del dato. Además, la cesión del modo que se pensó, permitiría, con la aplicación de nuevas tecnologías, crear nuevos datos e información personal. También, nótese que no se explica en el caso, cuáles serían las comunicaciones necesarias y obligatorias para hacer y por qué ello no es factible de hacerse desde los propios organismos (A.N.Se.S. y INSSJP).

La cesión y el uso de los datos, no quedan salvadas con la previsión en relación a que es válida la cesión entre organismos del Estado -junto a su garantía complementaria que todos los funcionarios están alcanzados por la obligación de confidencialidad y guardar secreto- dado que la información debe ser proporcional, razonable y adecuada. Verdaderamente, en muchas otras oportunidades hubo intercambio de información personal desde la A.N.Se.S. hacia otros Organismos estatales. Por tal razón, se generó la necesidad de regular la cuestión a través de la Resolución nº 952/2008 ya citada, sin embargo allí mismo se remarca que ello es factible siempre que lo sea en la medida del cumplimiento de sus funciones como no podría ser de otra manera.

A modo de ejemplo, obra a fs. 50/54, un Convenio de Intercambio Electrónico de Información entre la A.N.Se.S. y el Ministerio de Relaciones Exteriores y Culto cuyo objeto es *"…mantener actualizado el Padrón de Trabajadores y/o Beneficiarios del Régimen Previsional para los Funcionarios del Servicio Exterior..."*, de donde se desprende la pertinencia de la colaboración interestatal. En efecto, este Órgano Constitucional no niega que sea una práctica habitual, lo que sí en este caso no sería legal.

En el caso en estudio se trata de una transferencia que se observa masiva e indiscriminada y resulta por tanto inadecuada conforme la normativa vigente en materia de protección de datos personales. Además, no se ha probado ni dado una respuesta contundente sobre la existencia de ningún hecho excepcional o particular, tampoco existe un hecho público y notorio que habilite la necesidad de una comunicación direccionada, segmentada o especial por lo que la medida, en definitiva, es desmedida e impertinente.

En un caso español similar se ha dicho -en relación a la cesión entre organismos estatales- que *"Otra situación distinta de la anterior sería la derivada de que tanto el Área de Servicios Sociales del Ayuntamiento, como la Dirección de Servicios Sociales de la Comunidad Autónoma, pudieran ejercer competencias administrativas en materia de minusvalías, cada una en su ámbito territorial, y ello, con carácter general y con amparo en el artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal derivaría en que la sesión de datos entre ambas administraciones públicas sería lícita siempre y cuando*

esté justificada en la utilización de los datos para el ejercicio de las competencias administrativas en materia de servicios sociales como sería el reconocimiento, desarrollo y aplicación de las situaciones de minusvalía de los ciudadanos"[13].

También en el ya mencionado caso Halabi, del año 2009, la Corte Suprema de Justicia de la Nación, destacó la obligatoriedad de dar cumplimiento a los principios de proporcionalidad *"...c) que la aludida restricción resulte un medio compatible con el fin legítimo propuesto y d) que dicho medio no sea más extenso que lo indispensable para el aludido logro..."*[14].

Por otra parte, ante la posibilidad que la Secretaría de Comunicación Pública, utilice diversas modalidades de contacto con los individuos *"…que incluyen desde las redes sociales y otros medios de comunicación electrónicos, hasta el llamado telefónico o la conversación personal de forma de lograr un contacto individual e instantánea"*, hay que recordar que este accionar estatal resulta invasivo y podría tratarse de una práctica que incluso estaría opuesta a la legislación vigente en materia nacional (Ley nº 26.951 – Servicios de Telefonía - Registro Nacional "No Llame") y local (Ley nº 2.014 - "Registro No Llame").

Asimismo, hay que recordar que los Convenios habilitan la firma de nuevos acuerdos. Esta imprecisión en relación al uso de la información personal impide acordar con una utilización legal de los datos de los individuos de la Ciudad ya que se abren infinitas posibilidades en relación a su empleo. Por ello, esta Defensoría del Pueblo, advierte que los Convenios dejan fuera de la decisión a los titulares del dato y apelan de manera genérica a una necesidad de "comunicación" pero sin saber qué se quiere anunciar, cuándo se hará y/o cuándo se dejará de hacer. En el caso se observa que el/los organismos del Estado, deciden de modo subrogatorio un accionar sin la previa solicitud de autorización al legitimo titular del dato, dado que el Estado posee información personal en calidad de depositario, y es por ello una medida impertinente.

Por último, sobre la posibilidad o no de tratar datos de carácter sensible, hay que tener presente que hay una diferencia entre la ley local y la ley nacional de protección de datos personales, dado que la norma local es más tuitiva de los derechos de los individuos. El concepto de datos sensibles que da la ley local contempló la posibilidad de que cierta información personal, que en principio no sería sensible necesariamente, por su contexto se torne discriminatoria y, por tanto, sensible. Efectivamente, en

13 Guía de protección de datos personales para Servicios Sociales Públicos, APDCM, 2004, pág. 75/76.

14 Halabi, Ernesto c/ P.E.N. - Ley 25.873 – dto. 1563/04 s/ amparo Ley 16.986" file:///C:/Users/mgiorgelli/Downloads/09000006.pdf

el debate parlamentario de la Ley nº 1.845, se señaló respecto de la ley nacional que *"...3) Se mejoran muchos aspectos de la ley nacional que tienen defectos. Por ejemplo se aclara que el concepto de datos sensibles tiene carácter abierto y no cerrado, como cierta doctrina ha sostenido respecto de la ley nacional..."*[15].

En definitiva, el tratamiento automatizado de la información personal que habilita el/los Convenio/s, en concreto *"...herramientas que permitan instrumentar las políticas de la comunicación (…) destacándose la posibilidad de enriquecerlas, segmentarlas, clasificarlas y normalizarlas para posteriormente compartirlas con el organismo dador..."* no sería compatible con la protección del derecho a la intimidad. En esta dirección se ha dicho que *"El derecho a la intimidad puede ser definido como 'the rigth to be let alone' (derecho a ser dejado en la soledad de su espíritu) expresión acuñada por el Juez Cooley y posteriormente adoptada por juristas estadounidenses Warren y Brandeesis. Este concepto pretende una estricta protección legal de la persona, contra la publicidad de datos o de actos personales que se ponen en conocimiento del público, sin noticia o permiso de la persona afectada. Esta es la única que puede decidir qué es lo que se puede publicar o no..."*[16].

VIII.- Conclusiones finales

En el presente trámite se estudia el intercambio electrónico de información personal desde diversas bases que poseen la A.N.Se.S. y el INSSJP hacia la Secretaría de Comunicación Pública dependiente de la Jefatura de Gabinete de Ministros.

La transferencia electrónica de datos está admitida y por tanto regulada por la Resolución nº 952/2008 de la A.N.Se.S. En ella, se define la política de intercambio de información entre entidades externas y la A.N.SE.S. Allí, el art. 3º prevé en línea con la normativa de protección de datos que *"…el intercambio de información, a condición de razonable reciprocidad, o cuando lo fuere pertinente para el ejercicio de las funciones propias del Estado, en virtud de una obligación legal y todo previa evaluación de su factibilidad técnica, operativa y económica por parte de las áreas competentes…"*.

De las constancias del presente trámite, surge que los convenios no puntualizan qué bases de datos serán las transferidas, lo que habilitaría a la entrega de todo tipo de información. La A.N.Se.S. posee variada información personal en distintas bases destinadas a jubilaciones y

15 Despacho 1992 disponible en http://www.legislatura.gov.ar/

16 Ekmedkdjian, Miguel Ángel, Calogero Pizzolo (h) *Habeas Data El derecho a la intimidad frente a la revolución informática*, De Palma, 1998, pág. 8.

pensiones, sean estas contributivas o no contributivas, montos cobrados, datos relativos a los empleos de las personas e información familiar.

Estos datos relacionados entre sí o bien de manera individual pueden constituir datos sensibles, entendidos como aquellos que pueden generar algún trato discriminatorio a su titular (art. 3º de la Ley nº 1.845) como por ejemplo podría ser una pensión por discapacidad.

Por otra parte, los convenios habilitan a la firma de acuerdos por actas complementarias *"...que se consideren necesarias..."* (cláusula 3ª) a fin de complementar el contrato marco, lo que hace nuevamente necesario constatar el fin de la utilización de la información personal.

Como se expresara con anterioridad, el derecho a la protección de datos personales en el ámbito local encuentra amparo legal en el art. 16 de la Constitución porteña, y en la Ley nº 1.845 y su decreto reglamentario. Es evidente que el piso de esta Ciudad se amplió al instaurar la normativa, pero también en una batería de organismos con estabilidad legal y autonomía para intervenir en pos de la protección de los/as vecinos/as. En momentos en que ante el avance de las nuevas tecnologías se desdibuja el límite entre vida pública y privada, esta Defensoría del Pueblo cree conveniente garantizar que la eventual intromisión se realice en el marco de la ley que los Convenios no parecen asegurar.

En razón de ello, corresponde que esta Defensoría del Pueblo, se expida sobre el particular.

POR TODO ELLO:

EL DEFENSOR DEL PUEBLO
DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES
R E S U E L V E :

1) Exhortar al Director Ejecutivo de la Administración Nacional de la Seguridad Social (A.N.Se.S.), licenciado Emilio Basavilvaso, se abstenga de transferir la información personal de los/as vecinos/as de la Ciudad Autónoma de Buenos Aires, en el marco del Convenio aprobado por Resolución nº 166-E/2016 por contravenir los incs. 1 y 3 del art. 4º de la Ley Nacional nº 25.326

y el inc. 1 del art. 10 de la Ley nº 1.845.

2) Exhortar al Secretario de Comunicación Pública de la Jefatura de Gabinete de Ministros de la Nación, señor Jorge Miguel Grecco, se abstenga de hacer uso de los datos personales contenidos en las bases de la Administración Nacional de la Seguridad Social (A.N.Se.S.) de los/as vecinos/as de la Ciudad Autónoma de Buenos Aires.

3) Exhortar al Director Ejecutivo del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP), doctor Carlos Javier Regazzoni, se abstenga de firmar el acuerdo marco aprobado por Resolución nº 1005/2016 en relación a los/as vecinos/as de la Ciudad Autónoma de Buenos Aires.

4) Solicitar a la Secretaria Legal y Técnica de la Jefatura de Gobierno de la Ciudad Autónoma de Buenos Aires, señora María Leticia Montiel, informe:

a) cuáles son las fuentes que alimentan las bases de datos de la Administración Nacional de la Seguridad Social (A.N.Se.S.) y del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP);

b) para posibles casos futuros, notifique al Centro de Protección de Datos Personales de esta Defensoría del Pueblo, toda firma de convenio con la Nación destinada a la cesión de información personal por ser la autoridad de control de la Ley nº 1.845.

5) Solicitar al Director Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos de la Nación, doctor Eduardo Bertoni, que para casos futuros en los que exista compromiso de datos personales de vecinos/as de la Ciudad Autónoma de Buenos Aires, dé parte a esta Defensoría del Pueblo, por ser el Órgano de Control instaurado por la Ley nº 1.845.

6) Fijar en diez (10) días el plazo previsto en el art. 36 de la Ley nº 3 de la Ciudad Autónoma de Buenos Aires.[17]

17 **Ley 3, art. 36**: Con motivo de sus investigaciones, el Defensor o Defensora del Pueblo puede formular advertencias, recomendaciones, recordatorios de los deberes de los funcionarios, y propuestas para la adopción de nuevas medidas. Las recomendaciones no son vinculantes, pero si dentro del plazo fijado la autoridad administrativa afectada no produce una medida adecuada, o no informa de las razones que estime para no adoptarla, el Defensor o Defensora del Pueblo puede poner en conocimiento del ministro o secretario del área, o de la máxima autoridad de la entidad involucrada, los antecedentes del asunto y las recomendaciones propuestas.
Si tampoco así obtiene una justificación adecuada, debe incluir tal asunto en su informe anual o especial a la Legislatura, con mención de los nombres de las autoridades o funcionarios que hayan adoptado tal actitud.

7) Notificar, registrar, reservar en el Centro para su seguimiento y oportunamente archivar.

Código 432
CPDP
co/DCF/DGAL
Mlm/MAER/DMESA

RESOLUCIÓN Nº 1237/16
Vto. PEDUTO PARDO, Luis Eduardo
Director de Centro de
Protección de Datos Personales