LA PROTECCIÓN INTEGRAL DE LOS DATOS DE CARÁCTER PERSONAL EN MEXICO: LA INAPLAZABLE ELECCIÓN LEGISLATIVA, ENTRE EL MODELO NORTEAMERICANO Y EL MODELO DE LA EUROPA UNIFICADA

Francisco Javier Acuña Llamas

Sumario: *I.-Introducción; II.- El Renave y el Choicepoint, amenazas cumplidas al expolio de datos personales de la población mexicana; III.- Los nuevos registros públicos y privados (las SI's)[2] IV.- El Seminario Iberoamericano celebrado en Antigua Guatemala[1] y las "Reglas de Heredia" caminos a seguir. V.- La previsión normativa vigente en materia de protección de datos personales en México;VI A modo de conclusiones.*

I.- INTRODUCCIÓN

La iluminación del espacio público es una condición fundamental del medio democrático y se complementa con la ventilación de la atmósfera estatal, en una democracia moderna los ciudadanos tenemos derecho a estar bien, es decir al bienestar general y la calidad de vida de los habitantes de un determinado país radica entre otras cosas, en la calidad de la relación ordinaria que mantiene el ciudadano promedio con el Estado. Una vinculación razonable entre el ciudadano y el poder público sólo puede darse en un espacio saludable en el que la circulación constante de aire benigno sea fuente de la creatividad y el libre desarrollo de la personalidad de sus habitantes, y además el libre desarrollo de sus capacidades económicas, sociales y culturales.

La presente reflexión obedece a la necesidad de expresar el reclamo de una regulación adecuada para la protección de los datos personales en México ante el aparente desprecio o indiferencia del tema al seno del poder Legislativo (vacilación parlamentaria) que en realidad se explica por las grandes tensiones económicas que sostienen un reto de pulso y que han logrado paralizar la aprobación de una legislación que ineludiblemente tendrá que discurrir entre dos visiones opuestas pertenecientes a bloques perfectamente localizados: tanto el que representa y defiende las expectativas de la Unión

1 Seminario Iberoamericano sobre Protección de Datos Personales, evento celebrado en Antigua Guatemala del 2 al 7 de junio del 2003, la delegación mexicana estuvo integrada por el Senador Antonio García Torres y representantes del INEGI, de Banco de México y del IFAI; se presentaron 26 ponencias y la inauguración estuvo a cargo del Dr. José Luis Piñar Mañas, Director de la Agencia Española de Protección de Datos.

Europea viendo a México como un acceso natural a la región y a su vez como plaza de disputa con la Unión Americana en el terreno de la informática y la mercadotecnia directa; y del otro lado el punto de gravedad lo ejerce quien ambiciona y custodia de las intrusiones al mercado mexicano –en buena parte ya- cautivo del suyo, consecuencia del capítulo de dividendos que esa regulación habrá de transferir en exclusivo a la principal economía del NAFTA.

Las economías emergentes de la América Latina se aprestan a decidir a través de la implantación del sistema o modelo de regulación de los datos personales que adopten en breve una especie de certificación de identidad económica y financiera hacia uno u otro de los bloques en disputa, difícilmente las soluciones eclécticas resolverán para las economías emergentes una salida satisfactoria al respecto, o dicho de otra manera, si la intención consiste en adquirir una provechosa vinculación con Europa en términos de flujos comerciales se tendrán que observar las características del modelo europeo de tratamiento de los datos personales, que funciona como una verdadera cláusula de habilitación para fines de importantes parcelas de intercambio recíproco.

No puedo desconocer que también me alienta la oportunidad de referir el efecto que sobre la protección de los datos personales se ha podido registrar en relación a la incursión del Estado mexicano desde su ámbito federal de competencias en la senda de la apertura de la información pública gubernamental, en cuya ley se dedica un capítulo a la protección de datos personales en posesión de los poderes públicos y de otras entidades dotadas de relevancia constitucional, elenco que empero ha ingresado al tema de la transparencia informativa y del tema que nos ocupa con no pocas disparidades.

a) Hacia la sociedad de la información.-

La memoria magnética y el internet vinieron a insertarnos en la era de la "inseguridad digital". En la medida en que más aspectos de la vida personal y comercial se operan desde los ordenadores o computadoras es evidente que la informática y la telemática[2] se ha convertido en muy poco tiempo en un servicio de utilidad pública, aun contra la voluntad o entusiasmo de los usuarios a remolque, que empero han sucumbido a resistirse por el temor fundado a padecer las consecuencias de distanciarse de los mecanismos cibernéticos y quedar encofrados en una dimensión manual de la historia, la que los llevará a convertirse en una especie inadaptada para la comunicación cultural del porvenir.

Vivimos inmersos en una nueva era, la de las tecnologías y la aproximación virtual, en el mundo industrializado que nos ha tocado conocer, la competencia entre los estados nacionales continuará -y no falta quien profetiza, que- purgada de toda toxina ideológica y militar se reducirá a mera economía, en un marco de colaboración en el que el Mercado Común Europeo se muestra como modelo referencial[3] enfatizando la centralidad perdida de la cosa americana que ha encontrado diques a sus anteriores ventajas comparativas.

Las predicciones sobre la globalización sostienen que una vez más la tendencia imperante se irá estableciendo, los países marginales quedarán atrapados en la historia

2 Mientras la informática es la ciencia del tratamiento automatizado o electrónico de la información, la telemática es la unión de la informática con las telecomunicaciones Cfr obra colectiva Jijena Leiva Renato, Andres Palazzi Pablo y Téllez Valdes, Julio en El Derecho y la sociedad de la información: la importancia de internet en el mundo actual coedición Tecnológico de Monterrey campus Estado de México-Miguel Angel Porrua, México 2003.

3 Cfr Mercader Uguina, Jesús R, en Derecho del Trabajo. nuevas tecnologías y sociedad de la información, Valladolid, Espana, Editorial Lex Nova, , 1° edición 2002, pagina 25 y sigs.

sumergidos en las tensiones étnicas (el África negra que se hunde en solitario en la hambruna y las pandemias) y /o en las pasiones sectarias síntoma típico de las regiones sentimentalmente resistentes a la nueva era convertidas en submundos, periferia de la nueva época, en la que sin embargo participarán de modo recipiendario, nunca equivalente, y los efectos perjudiciales son y serán sin duda para los más desposeídos de esas poblaciones.[4]

Ante las nuevas tecnologías se achica el orbe mientras crecen las nuevas amenazas que se ciernen sobre la humanidad entera y que bajo el efecto mariposa (la repercusión global de lo aparentemente insignificante que ocurra en cualquier parte) empujan a lo que llamamos nuestra civilización a *la era del vacío*[5] y que otros con cierto matiz han denominado *la sociedad de riesgo.*[6]

Un dato adicional de esta sociedad de la información a la que sin duda avanza la civilización occidental se refiere al proceso gradual mediante el cual el Estado democrático moderno ha digitalizado el seguimiento y programación de todas sus actividades y además ha venido delegando en manos de los particulares una serie de potestades públicas, –translación legalizada- fenómeno que no deja de suscitar enormes replicas y al que se le conoce también como la "despublificación" y que entraña nuevas incógnitas ahí donde se producen el peligro de incrementar con ello el riesgo del derecho a la privacidad de los ciudadanos entre otras y diversas afectaciones a la sociedad.

De manera esquemática, podemos aquí reproducir[7] las tensiones más comunes que se suscitan entre los derechos a la información y a la privacidad y del consumidor:

Mientras –en positivo- el derecho a la información facilita tareas, la vida en sociedad, elimina costos superfluos, elimina la intermediación, se dice –en negativo- deja pocas esferas reservadas y hace más vulnerable al hombre.[8]

Se afirma en positivo, que personaliza la atención, mejora la salud, permite orientar el mensaje, saber con precisión que quiere la ciudadanía, permite mejorar la seguridad al producir un conocimiento de los rastros y registros, en materia de salud pública facilita el acceso oportuno en caso de accidentes, favorece la elaboración de políticas públicas para el control de las epidemias, desde la Economía facilita el acceso al crédito, baja la morosidad, facilita la estadística, anticipa problemas, mejora la recaudación impositiva, incrementa el comercio y orienta la publicidad a los destinatarios adecuados, etc.

En negativo se aduce[9]: Despersonaliza la atención, invade la intimidad y favorece al hipercontrol estatal, incrementa el riesgo de que el mensaje sea manipulado, afecta la seguridad individual al incrementar el riesgo de que otros (estado y o particulares) accedan a los datos íntimos, se puede llegar a conceder un excesivo control del estado o de otros particulares sobre datos personales: ingresos, situación económica, situación fiscal, etc.

---

4 Cfr Escohotado Antonio, en Caos y orden Madrid, Espasa Calpe, 1999.

5 Cfr Mercader Uguina, op,cit.

6 Beck, Risikogesellschat, 1986, citado por Rivero Ortega Ricardo en el estado vigilante, Madrid, Tecnos, 2000, pagina 26.

7 Cfr V.Lynch, Horacio Maria, "Notas sobre el Derecho en la Era Digital"en La LEY, Ano LX, Nro 93, 15 de mayo de 1996, citado por http://www.it-cenit.org.ar/ Publicac/ PeopleBases/Investigac5.htm

8 Ibídem.

9 Ibídem.

Por ello entendemos que la mejor visión sobre las hipotéticas tensiones que indudablemente provoca el tema se debe zanjar desde una observación de conjunto, nunca desde un mirador maniqueo, tampoco se pueden anticipar, como arriba lo reproducíamos, todos los escenarios en positivo o en negativo, el asunto reclama una conciliación de ventajas relativas con las inconveniencias probables y siempre intentando un ejercicio virtuoso.

b) El aparente dilema entre la apertura y la custodia de los datos personales

Ahora que en México estamos abriendo claraboyas y tragaluces en los sótanos estatales (tras la aprobación de la Ley Federal de Transparencia y Acceso a la Informacion Pública y de 16 leyes similares de las 32 entidades federadas) es inevitable hablar de la tensión que siempre existirá entre apertura de la información pública y la custodia de los datos íntimos de la población. Los datos personales que guarda el Estado en sus cajones y armarios representan uno de los asuntos más delicados de su responsabilidad, el síndrome de la apertura informativa encuentra una excepción en el manejo y resguardo de ciertos datos personales de los habitantes que posee el Estado en sus archivos, los datos más sensibles sobre las personas (origen o pertenencia étnica, religión, aficiones, salud, preferencias sexuales etc.) merecen una protección reforzada.

El proceder público debe ser recto y correcto y sólo los controles externos obligan a los servidores públicos a comportarse debidamente en beneficio de la población ¿pero cómo asegurar eficacia y honradez si el oficio del servicio publico se hace en penumbras? La creación del Instituto Federal de Acceso a la Información Pública, el IFAI, nos acerca a encontrar una ruta hacia la transparencia de la información gubernamental, toda vez que es el Poder Ejecutivo el que más contacto mantiene con la ciudadanía mediante la prestación de los servicios públicos, trámite que independiente de la calidad de dichos servicios exige inevitablemente el manejo de un océano de datos personales que cada dependencia involucrada requiere, obtiene, acumula, traspapela, recupera ... para diversos procesos burocráticos ligados a la satisfacción de tales necesidades sociales.

La dimensión de esta diaria relación del ciudadano con la red capilarmente tejida de las ventanillas públicas en los tres niveles de autoridad en las que como picaporte entrega sus datos individuales es impresionante; las más visibles por la magnitud de los bancos de datos corresponde a ciertas entidades que refieren registros transversales que prácticamente abarcan a la mayoría de los habitantes, el Registro Civil y el Registro Público de la Propiedad, el fisco, los servicios masivos de la atención médica popular, los que importan al cómputo del derecho a las prestaciones laborales como la vivienda, el sistema para el ahorro, pensiones y jubilaciones, los bancos de datos del sistema nacional de población y del sector educativo, etc. Sin embargo, no son esas las únicas fuentes de recolección de datos personales a gran escala, otra gama de servicios públicos precisa de datos personales para toda clase de solicitudes, lo mismo los beneficiarios de programas de ayuda económica y en especie a los más desfavorecidos, que los que reflejan destinatarios de aprovechamientos y derechos derivados de permisos y concesiones públicas, es más, todo trámite, por simple que parezca, conlleva la recolección de datos personales y algunos de ellos datos "sensibles" o íntimos.

En los regímenes autoritarios el solar nacional se convierte en un bosque sombrío, la metáfora nos indica que el bosque se forma por la mala hierba del voluntarismo y la arbitrariedad que impide la luz y acostumbra a los ciudadanos a caminar sorteando obstáculos entre las sombras.

La eficiencia gubernamental insinuada – como presupuesto- mediante la operación del derecho ciudadano al acceso a la información pública, alivia muchas de las frustraciones del ciudadano común que, en un contexto de opacidad, vive la amargura de padecer las más variadas formas de despotismo, maltrato e indiferencia por parte de funcionarios públicos exentos de control alguno obran a su modo favoritos de la discrecionalidad total, la impotencia de los habitantes que padecen esa situación asfixiante, suele producir en ellos paranoia y desde luego una vocación de ruptura con lo establecido. Curiosamente, aún en el Estado democrático que procede en muchos de sus actos en vitrina, también se puede dar el caso de que por ineptitud o corruptela se viole la confidencialidad de los datos personales que tiene a su resguardo y que se filtre al mercado o a la prensa ese tipo de datos. El escandaloso e inaclarado caso de la venta de las copias de las bases de datos del Registro Federal Electoral a la compañía estadounidense *Choice Point*, ocurrido en el 2002 nos revela el peligro que corremos como ciudadanos cautivos de movimientos desautorizados de datos personales para fines de lucro y especulación comercial.

Un enfoque incorrecto de la apertura informativa podría llegar a representar costos y riesgos altísimos al derecho a la intimidad de las personas, a la privacidad de aquellos ámbitos de la vida de cada quien y que solo a cada uno de nosotros corresponden. Los datos de la vida privada son un patrimonio intangible de los ciudadanos (personas físicas) también de las personas morales y sin duda de los mismísimos funcionarios públicos.

Así las cosas es preciso acotar: transparencia y apertura sobre los datos públicos, toda la posible (porque sin haber con ello un conflicto siempre habrá información reservada y confidencial) y urgente que el acceso a la información extinga el tabú de los ciudadanos de atreverse a preguntar todo lo concerniente a la plaza publica, que hasta ahora ha sido más que tratada como una concesión aislada de los funcionarios que han vivido bajo el sugestivo dogma de que "la información es poder" y que los hizo por largo tiempo favoritos de ese viejo sentimiento de dominio sobre el cargo y sus efectos, patrimonialismo del puesto público que ejercen.

La calidad de vida en una democracia exige un conjunto de satisfactores que solo se pueden dar si la conducción pública es presumiblemente recta (razonablemente honrada) y correcta (oportuna, segura y justa) lo que hace que la inferencia sobre la función del Estado de Derecho sea veraz.

El núcleo duro del problema de la protección efectiva de los datos personales debe plantearse desde la visión de Guillermo Consentino cuando afirma que l*a existencia de bases de datos en el ámbito del Estado llamadas por su ubicación "públicas" y bases de datos en manos de personas u organizaciones privadas o no estatales, denominadas, siguiendo el mismo criterio "privadas", no necesariamente cambia la condición de los datos personales que puedan contener y no disminuye el nivel de protección que la ley les asigna.*[10]

El supuesto dilema entre la apertura informativa y la protección adecuada de los datos personales de la población se supera cuando se logran ambas condiciones perfectamente complementarias y jamás antagónicas, pero acaso vale la pena referir que normalmente la regulación de ambas ha sido simultánea o inclusive primero se ha resuelto el problema de la protección de los datos personales y luego se ha efectuado la elaboración del marco normativo e institucional de la apertura informativa (que demanda el ejercicio ciudadano del acceso a la información pública), sobre este punto en México

10. Guillermo Cosentino, 'La información judicial es pública pero contiene datos privados, como enfocar esta dualidad', en Internet y Sistema Judicial en América Latina (en prensa).

como en tantos otros casos de la incorporación de instituciones jurídicas o de las herramientas y mecanismos para el desarrollo de las mismas estamos haciendo las cosas sin seguir un método consistente que se inspire en el Derecho Constitucional Comparado. El tiempo lo consignará y los reproches y lamentos habrán de servir de poco.

c) Sin regulación pertinente la incertidumbre permanece.

La alternancia de la clase política al frente de la responsabilidad ejecutiva federal y la corresponsabilidad legislativa de un Congreso dividido en el que ningún partido alcanza la mayoría suficiente, además de la torpeza y la falta de una previsión y de un "sentido constitucional de Estado"[11] –de la clase política en su conjunto- para dimensionar las cuestiones de gran trascendencia de las ordinarias ha cobrado sus lastres en materias tan sustantivas como ésta.

Y mientras transcurren los días del estancamiento político, el ciudadano que protagoniza de alguna manera en el medio público (cualquiera que sea su rama, mensaje o misión), sigue su ruta sobre la cuerda floja de una seguridad jurídica reducida a niveles de precariedad.

Los viejos hábitos del gobierno espía persisten. ¿A dónde van las grabaciones de las conversaciones telefónicas de cierto sector social (seria un despropósito suponer que las de todos pero sí de quienes circunstancialmente juegan un papel importante en la sociedad)? Y es que es grave la inferencia como la respuesta, sabemos[12] –como un lugar común- antes efectuaba el Centro de Inteligencia y Seguridad Nacional[13] (CISEN) y lo peor, ahora alguien las sigue efectuando desde adentro del gobierno o desde afuera sin mediar autorización judicial. Por supuesto que completas o fragmentadas dichas conversaciones son un registro indebido que debe localizarse y destruirse.

Y también las imágenes de nuestro rostro o de cuerpo entero mientras participábamos en una marcha de protesta o hacíamos antesala en alguna oficina pública o en cualquier otra faceta de nuestra vida privada, filmaciones o fotografías efectuadas a través de informantes del Gobierno que luego se guardan en algún estante oficial, en fin imágenes tomadas sin nuestro consentimiento mientras ingresábamos o salíamos de determinando lugar de culto, centro nocturno, espectáculo, sólos o acompañados, y así

---

11 Sentido constitucional de Estado es una frase que invoca todo un campo de comprensión, refiere una actitud frente al significado de integrar una nación ceñida a la Constitución a modo de un compromiso individual y grupal mezclado de visión de futuro y sentimiento cívico político propio de demócratas, que se manifiesta en acciones sistemáticas dirigidas al propósito fundamental de vivir dentro de la Constitución, o lo que es lo mismo a la permuta de lo anterior por hábitos ciudadanos y funcionariales de corte democrático demostrables, comprobables.

Se debe dejar para el ayer esa gama de soluciones públicas (de la Polis) tanto políticas como sociales e individuales que lastraron nuestra identidad ciudadana y nos programaron / adiestraron a vivir en una democracia "orgánica", conducible, manejable a base de la zanahoria y la vara, al calor de la simulación necesaria para justificar premios o castigos ajurídicos: impunidad al fin de cuentas, complicidades, fortunas indebidas de actores políticos y sociales y pobreza extrema popular.

O nos volcamos a salvar lo alcanzado en términos de la modernización democrática que ha tocado positivos aspectos del ordenamiento jurídico y ha prohijado un nuevo elenco institucional en marcha o veremos escenarios de estancamiento y hasta regresión por la incapacidad de los actores públicos de aportar un extra de esfuerzo por encima de sus aspiraciones y ambiciones partidistas, es mucho lo que hay que hacer para contornear la democracia constitucional que aún no tenemos. La aventura democratizadora ha sido costosa y conveniente también, pero la fragilidad de nuestras convicciones democráticas nos advierten peores riesgos y peligros, más caros a la postre si no armonizamos la incidencia cultural cívico-política de las nuevas herramientas para la corrección de los excesos del acto público en beneficio de la sociedad.

12 Sirva aquella sutil pero implícita aseveración que dice: -yo no lo sé de cierto, lo supongo-.

13 Órgano perteneciente a la Secretaría de Gobernación del gobierno federal, típico instrumento de inspección autoritaria.

toda clase de filmaciones y o fotografías sobre aspectos de la vida íntima de ciudadanos (encuentros o reuniones en domicilios particulares etc.) son un material delicadísimo que entraña datos personales y un reflejo de esa costumbre añeja de *los imperantes y su séquito* de acumular información privada de los críticos o disidentes del régimen para fines inconfesables, de potencial utilidad[14] extorsiva.

La calidad de vida en democracia no solamente se demuestra en el Producto Interno Bruto, cifra que en las sociedades desiguales –como la nuestra- representa los descomunales ingresos de unos cuantos y que, para efectos de la estadística aritmética, se adicionan a los ingresos de los que poco ganan y que se atribuyen a la población como un promedio simbólico que dice muy poco en el lenguaje de la microeconomía.

En el reciente encuentro internacional del Movimiento Mundial para la Democracia celebrado en Durban Sudáfrica, una de las denuncias fue precisamente la de mantener la mirada en la realidad micro de las regiones para interpretar correctamente los impactos de la calidad de la gestión pública sobre los ciudadanos.

II.- EL RENAVE Y EL *CHOICEPOINT*, AMENAZAS CUMPLIDAS AL EXPOLIO DE DATOS PERSONALES DE LA POBLACIÓN MEXICANA.

El mercado y sus leyes han construido redes de circulación incesante que hace reconocer que el insumo por excelencia lo son los datos personales de clientes y proveedores actuales y potenciales y ahí en el mundo de las empresas privadas también se diseñan enormes bases de datos para toda suerte de estrategias propias de la comercialización de productos y bienes de servicio, en la era de la mercadotecnia y las telecomunicaciones casi todo pasa por la cibernética y los peligros de un uso inconsulto e indebido de cierta información relacionada con datos íntimos de usuarios o beneficiarios es uno de los grandes temas de obligada deliberación parlamentaria para la actual legislatura. ¿qué pasó realmente con los datos personales que se recogieron por el truncado experimento del RENAVE (Registro Nacional de Vehículos)[15] y como fue que se comercializó con los datos personales del cóctel de bases de datos públicos servidos al *Choice Point*?

La ausencia de una legislación de la materia en México no es óbice para efectuar las investigaciones pertinentes y la localización de los responsables que en cada caso, guardadas las proporciones, expusieron a serios riesgos el derecho a la intimidad de los particulares que confiaron sus datos a autoridades concretas.

En el caso del RENAVE se deben fincar responsivas por negligencia institucional a quienes para tal objeto requirieron datos personales acompañados del pago del respectivo servicio de registro. Que, dígase de paso, dichos recursos no se han reinte-

14 Sirva como mera referencia las revelaciones escandalosas de las filmaciones efectuadas por el gobierno de Alberto Fujimori a quienes eran sobornados por sus propios agentes y almacenados como materiales de chantaje selectivo..

15 Registro Nacional de Vehículos, puesto en marcha por decreto presidencial en 1999 y concesionado a particulares para operar mediante el cobro de una cuota por la adquisición de vehículos nuevos, que finalmente fuera cancelado en agosto del 2000 tras la detención e inicio de procedimiento de extradición a España de Ricardo Miguel Cavallo, su entonces director, relacionado con los crímenes de lesa humanidad cometidos por la dictadura argentina en la década de los setenta, sobre este tema Véase en extenso de GUEVARA B, José Antonio " México frente a la jurisdicción universal: La extradición de Ricardo Miguel Caballo" en Revista Mexicana de Derecho Público, N° 3, abril de 2002, México, ITAM, Departamento de Derecho.

grado a sus emisores y que debería de añadirse la suma de dicho concepto una especie de reparación económica simbólica al agravio causado por el Gobierno por la exposición innecesaria al riesgo de un uso indebido de tal información en parte confidencial, que tras la detención del entonces director recientemente extraditado a España y al suicidio de un alto funcionario del Gobierno Federal de la entonces Secretaría de Comercio, fuera cancelado sin más el malogrado RENAVE que nunca se debió haber configurado como una concesión a particulares.

En efecto, sólo un juez podría fincar al Gobierno federal la obligación de una indemnización a las víctimas de tales agravios por el hecho de haber sido obligados a un pago de lo indebido y colocados en una situación de vulnerabilidad en cuanto al derecho a la privacidad, pero, que se sepa, los miles de ciudadanos que pagaron al RENAVE el importe de referencia no se han agrupado para efectuar sus reclamaciones por la vía judicial, acaso algunos lo hayan hecho de manera individual pero serán los menos porque la cuantía del pago efectuado objeto de la reclamación de la reparación del daño es realmente inferior a los costos de enderezar un juicio de modo aislado, no así, el ingreso que tuvo la hacienda federal si se contempla el monto global de lo recaudado.

La Comisión Nacional de Derechos Humanos podría haber intervenido investigando la negligencia institucional de comentario y sobre todo fincando un precedente hacia el respeto al derecho a la intimidad de las personas afectadas, recomendando en su caso al Ejecutivo Federal acciones –aun simbólicas- de carácter compensatorio para aliviar el agravio de la exposición a los riesgos nada irreales si se constata y se conectan con el reciente escándalo del *Choicepoint*, cuya evidencia hace prueba plena de la ineptitud funcionarial (ausencia de medidas efectivas para la custodia de información confidencial) y ligereza para asegurar mínimos de protección a bienes intangibles como los que refiere el derecho a la intimidad de las personas.

En el caso del *Choicepoint* la gravedad de la cuestión es aun mayor porque en principio la ciudadanía entera tiene derecho a saber qué bases de datos se filtraron al mercado y el inminente ejercicio de responsabilidades a los funcionarios involucrados por la negligencia institucional de poner en riesgo el derecho fundamental a la intimidad de los millones de personas enlistadas en tales bancos de datos vaciados literalmente a las manos de los dueños del *Choicepoint*, mediante conductas delictivas que pusieron a los titulares indeterminados de dichos datos en toda suerte de peligros.

A la fecha –que se conozca- no se han querellado ciudadanos concretos ante los tribunales competentes contra las instancias públicas de las que se fugó en copia dicha información, en este caso es más difícil acreditar la afectación directa de los querellantes porque no se cuenta con la certeza de quiénes resultaron expuestos por tales hechos de tremenda irresponsabilidad gubernativa, por ello sería a su vez nuevamente imprescindible que la Comisión nacional de los derechos Humanos efectuara una investigación para que a través de recomendaciones específicas señale al Ejecutivo Federal medidas urgentes para que se sigan las investigaciones y se lleve a juicio a los responsables y especialmente para asegurar la inviolabilidad de los datos personales en posesión de la Administración Pública Federal, sin perjuicio de que la Ley Federal de Transparencia y Acceso a la Información Pública encomienda al IFAI (instituto Federal de Acceso a la Información Pública) a emitir lineamientos para la protección de datos personales.

La CNDH también podría y debería instar al Congreso de la Unión a la elaboración de una ley para la protección de datos Personales y en lo inmediato que su decidida actuación al respecto haga sentir a la población entera el efecto protector del Ombudsman Nacional que es por definición constitucional el máximo Defensor de los derechos humanos por la vía no jurisdiccional y por ello irremplazable para intentar la

restitución posible de los bienes jurídicamente tutelados a favor de los afectados por la violación de tales derechos, en situaciones que, como ésta, exhiben deficiencias estructurales conculcatorias de los derechos a la privacidad e intimidad de las personas que si no admiten una reparación concreta sí una denuncia categórica y una corrección profunda del ejercicio público.

a) La ruta del escándalo de la venta del padrón electoral del IFE al Choicepoint

- La mañana del 13 de abril del 2003 el rotativo Reforma de México expone en su primera página "Adquiere EU listas del IFE" (Instituto Federal Electoral) se detalla que la empresa Choicepoint realizó la adquisición del padrón electoral y de bases de datos de licencias para conducir del Distrito Federal y cuestiona la legalidad del asunto; el 17 de abril en el mismo periódico se revela que Choicepoint ofrece a través de su sitio de internet acceso a información crítica.
- El 18 de abril Reforma señala que mientras que el Código Federal de Instituciones y Procedimientos Electorales establece que los datos proporcionados por los ciudadanos al Registro Federal de Electores son confidenciales, al menos cuatro mil funcionarios partidistas y electorales cuentan con atribuciones para acceder a esos expedientes, es decir, subraya "la misma ley abre la puerta para que diversos funcionarios dispongan del padrón".
- El IFE matiza, "tienen acceso al padrón 11 partidos políticos con registro, 32 autoridades electorales en las entidades federativas y el comité técnico del padrón electoral"; el director del Registro Federal de Electores (RFE)Alberto Alonso y Coria informa dos acciones concretas, intentarán verificar la destrucción del padrón electoral mexicano por parte de Choicepoint, para lo que se realizan gestiones diplomáticas a través del Consulado de México en Atlanta, en atención al los hechos se cancela el convenio de colaboración entre Secretaría de Gobernación[16]-
- Registro Nacional de Población y el Registro Federal de Electores del IFE; el DR. Julio Téllez Valdés fue citado por la Fiscalía Especial para Delitos Electorales (FEPADE) de la PGR[17] en calidad de perito y declaró que a consecuencia del vacío legislativo en materia de protección de datos personales es que permanece y aumenta el riego de cruza o interconexión de bases de datos y otros efectos negativos derivados de la no prohibición de algunas de esas prácticas cuando afectan a datos personales sensibles.

Cabe señalar como antecedente que el 5 de agosto de 1998, el entonces Presidente del IFE, José Woldenberg instruyó presentar ante la FEPADE una denuncia contra GM Group (Aurora Ohio), la que resultó improcedente, otra denuncia presentada por el IFE en el año 2002 contra una firma mexicana tampoco procedió, en cambio fue la denuncia 155/FEPADE/2003 la que sí se consideró procedente, indagatoria que se encuentra actualmente en curso.[18]

16 Ministerio del Interior.

17 Procuraduría General de la República (equivalente a la Fiscalia General).

18 El director del Federal de Electores, Alberto Alonso y Coria, afirma que intentan verificar la información sobre la destrucción del padrón electoral mexicano por parte de ChoicePoint.19 También afirma que se ha cancelado el convenio de colaboración entre SEGOB-RENAPO y RFE contacta a FEPADE-PGR y al Consulado de México en Atlanta.

El único de los consejeros del IFE que hizo de ésta cuestión un reclamo de llegar a fondo fue Jaime Cárdenas Gracia quien protestara en repetidas ocasiones a la contraloría interna al no querer aquella revelar el nombre de la empresa mexicana que compró la base de datos del Padrón Electoral.[19]

- La PGR realizará su propia investigación sobre el caso, la empresa Choicepoint entregó a la PGR 10 discos compactos con base de datos que habían adquirido y que incluye información de 58 millones de mexicanos.[20]
- Funcionarios del gobierno federal reconocen que la venta del padrón electoral y otras bases de datos ha puesto en riesgo la seguridad nacional, al vulnerarse sistemas de informáticos de la nación e información estratégica ChoicePoint pagó por cada base de datos alrededor de 500 mil pesos. La agencia federal de investigaciones (FBI) la agencia Antinarcóticos (DEA) El Buró de información y la aduana del departamento de seguridad interior, entre otros, utilizan para recabar antecedentes de delincuentes, esa información[21]
- El FBI elaboró un documento marcado como "secreto" dirigido a las agencias de seguridad nacional donde da el visto bueno para utilizar información de la empresa ChoicePoint. A dos años de haberse redactado el memorando y después del escándalo continental que provocaron los métodos de obtención de informa-

---

Reforma página 11 sección A18 Abril 2003. Atribuyen los abusos a falta de legislación Lamenta el Dr. Julo Téllez Valdés la no aprobación de la ley de datos personales en 2001. Indica riesgo de no prohibir cruza o interconexión de bases de datos. Y otros efectos negativos derivados del vacío legislativo.El Dr. Téllez fue llamado por la PGR a declarar como perito en el caso.

Reforma página 11 sección A19 Abril 2003. Sugiere anular en EU uso de padrón electoral. Los consejeros electorales manifestaron demandar a autoridades de EU la anulación del contrato de compra -venta del padrón electoral.El tema de la venta de información del padrón a una empresa de EU, permeó en las discusiones de los pasillos del IFE cuyo Consejero General celebró una sesión especial.

Milenio página 10, 1 Mayo 2003. Detectan a quien vendió el Padrón a ChoicePoint. El IFE confirmó que el gerente de sistemas de una empresa mexicana adquirió una base de datos que contenía información confidencial sobre millones de mexicanos y posteriormente estos datos los vendió a CholcePoint. Se habla de que la persona que vendió esta información pudo haber sido un ex funcionario del IFE

La Extra página 10, 27 abril al 3 Mayo 2003 ChoicePoint y la Violación de la Soberanía Nacional. Desapareció buena parte del padrón electoral, y se encontró tiempo después en Atlanta EU en la empresa ChoicePoint esta empresa promueve la venta de datos confidenciales.De manera misteriosa desapareció buena parte del patrón electoral, y se encontró tiempo después, en la empresa espía de EU ChoicePoint. En nuestro país corrieron las acusaciones, mientras que el verdadero culpable está libre dispuesto a corromper a otra autoridad.

19 "el IFE debe presentar una denuncia ante tribunales federales" palabras del Consejero Jaime Cárdenas quien asegura que Jonathan Davis, presidente la Comisión Nacional Bancaria y de Valores se ha burlado del IFE ya que no entrega oportunamente la información que requiere el instituto para profundizar en investigaciones

20 Milenio, página 4 del 17 Mayo 2003, ChoicePoint entrego el Padrón a la Procuraduría General de la República.La entrega de discos se llevó a cabo en Consulado de México en Atlanta, donde los empresarios de ChoicePoint rindieron su declaración sobre compraventa de esa información Conclusión a la que llego el IFE en sus investigaciones: único responsable, Juan López Bedolla. La funcionaria de la PGR recordó que la Fepade no puede determinar la presunta culpabilidad de alguna persona.

21 Milenio10 junio 2003. El IFE clasificó como confidenciales seis rubros El IFE restringió seis rubros de la información electoral del país que liberaría. Su nueva Unidad de Enlace determina que no está clasificada como reservada o confidencial. El acuerdo está estipulado en doce hojas en donde se presenta la determinación de agregar otros seis rubros a las trece áreas a la información que también se reserva en la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental. El consejero presidente y sus decisiones serán supervisadas por tres personas.

Milenio17 junio 2003. A petición de Choicepoint, la PGRLa Fiscalía Electoral de la República determinó destruir la base de datos que empresarios mexicanos vendieron a la firma estaunidense. Solicitaron al vicepresidente internacional de ChoicePoint, Paul Butting, vía Internet luego por notificación judicial bajo protesta de decir verdad que se abstendrá de guardar sus archivos una copia de citada base de datos.

ción de ChoicePoint en una decena de países de América Latina, incluidos México, Colombia, Costa Rica, Brasil y Argentina, EPIC sostiene que es más importante que nunca normar y transparentar el uso de información pública[22]

- La información de ciudadanos mexicanos obtenida por la empresa estadounidense ChoicePoint que está en manos de la CIA y del FBI podría ser utilizada en Enchanced Promis, el programa de software más complejo que se haya diseñado con los fines de espionaje. Este programa pudo realizar búsquedas simultáneas y fue creado para la utilización de los servicios de inteligencia del aquél país[23]
- Funcionarios Argentinos de procuración de justicia se dirigieron preocupados de ChoicePoint utilice la lucha contra el terrorismo como pretexto para ofrecer a gobiernos informes de millones de latinoamericanos con fines de control político. El Departamento de Seguridad Doméstica de Estados Unidos sí revisó la información sobre ciudadanos mexicanos proporcionada por ChoicePoint. Esto resulta aún más probable si se considera que EU ha violado reiteradas ocasiones las reglas del derecho internacional.
- El Secretario de la Comisión de Puntos Constitucionales de la Cámara de Diputados, exigió al gobierno federal promueva candados que garanticen la seguridad de datos confidenciales, y evitar filtraciones fuera del país.
- Choicepoint cerró la puerta a la FEPADE. En abril la Fepade empezó a indagar sobre el robo del padrón electoral mexicano. Se comprobó que fue comprobado por ChoicePoint, firma dedicada a vender bases de datos para el gobierno estadounidense y empresas de ese país, las autoridades de la Fepade se regresaron a México sin verificar que la información hubiera desaparecido de todas las computadoras de la compañía, como lo aseguró en un comunicado ChoicePoint[24]
- El gobierno mexicano se vio orillado a solicitar al Departamento del Justicia de Estados Unidos que intercediera para que la Fepade pudiera verificar la destrucción del padrón electoral, sin que a la fecha tengan respuesta. Advierte SER que seguirá expedición de matrículas. La Secretaria de Relaciones Exteriores (la cancillería) advirtió que México continuaria expidiendo matrículas consulares en EU porque el derecho internacional así se lo permite, y aseguró que los requisitos para otorgar dichos documentos y su impresión cumplen con estándares de seguridad mundial.
- Al terminar mayo del 2004. El asunto permanece inaclarado y el curso de la investigación no puede excluir de las responsabilidades que les correspondan al anterior Consejo del Instituto Federal Electoral.

---

22 El Independiente 1A26 Junio 2003. El padrón Electoral usado en la guerra contra el terrorismo ChoicePoint espió para Washington. EU compró el padrón electoral y por lo menos cuatro bases de datos más que pertenecen al Estado Mexicano, en una operación en la que ChoicePoint actuó como brazo de inteligencia Para garantizar la seguridad de su territorio frente al terrorismo internacional, EU compró el padrón electoral y por lo menos cuatro bases de datos que pertenecen al Estado mexicano, en una operación en la que la empresa ChoicePoint actuó como su brazo de inteligencia.

23 El Independiente 6ª, 27 Junio 2003.La base de datos ofrecida por ChoicePoint, inútil, aseguran EU admite que reviso el padrón. La información que obtuvimos sobre México era completamente inservible información que nadie necesitaba. El Departamento de Seguridad Domestica (DHS) tuvo acceso a información sobre datos mexicanos proporcionada por la empresa ChoicePoint, sin embargo era completamente inservible.

24 Reforma 1 A del 27 Junio 2003. Desacredita el FBI matrícula consular El FBI y el departamento de Justicia de Estados Unidos consideraron que la matrícula consular mexicana podría ser un elemento que facilite el terrorismo, ya que la matricula puede ser En México, la Secretaría de Relaciones Exteriores respondió anoche a las críticas del funcionario del FBI sobre la matrícula consular, y aseguró que los requisitos para otorgar dicho documento y su impresión cumplen con estándares de seguridad

Reforma 21 A27 Junio 2003.

b) El fincamiento de responsabilidades a los cuatro detenidos del caso *Choice Point*, otro error gubernamental.

El yerro de la Fiscalía Especial para Delitos Electorales de la Procuraduría General de la República al acusar ante el Juez de Distrito (juez federal de amparo) a los cuatro presuntos responsables de la sustracción de las bases de datos de comentario bajo la modalidad del delito de "traición a la patria" una cortina de humo al asunto.

A guisa de lo anterior no admite réplica la afirmación que hacemos de que las bases de datos en posesión del gobierno, deben ser custodiadas bajo siete llaves, pero no concentradas dichas bases de datos en un mismo lugar sino en cada una de las entidades públicas que almacenan datos personales sensibles de la ciudadanía.

Ahora se sabe –dichas bases de datos- se filtraron desde el Registro Nacional de Población dependencia de la Secretaría de Gobernación. Con rigor se antoja preguntar ¿qué hacían las bases de datos del padrón del IFE organismo constitucional autónomo dentro del ministerio del interior del Ejecutivo Federal? y ahí mismo junto con las del Servicio Postal Mexicano que fueron sustraídas, se dice en 1999 y naturalmente la respuesta que se ha dado es que estaban ahí las bases de datos del Padrón Electoral burlado para los efectos de elaborar la Clave Única de Registro de Población (CURP), pero claro está sin haberse tomado las medidas precautorias.[25]

El asunto exhibe negligencia institucional o lo que es lo mismo cuando, por omisión indolente, o corruptela, o ambas, falla la cadena de dispositivos para prevenir que los errores institucionales de la administración pública produzcan graves consecuencias y en éste caso se puso en condición vulnerable el derecho a la privacidad de cada uno de los titulares (millones) de los datos personales transferidos y vendidos al *Choice Point*; fueron dos situaciones, el asalto y el tránsito ilegal de esos bancos de datos personales.

Los hechos delictivos de comentario son graves y reprobables pero de ahí a encuadrarlos en actos deliberados de traición a la patria fue una burda medida extrema, más efectista que razonable, por ello el Juez Federal decidió el 24 de diciembre 2003 encuadrar las acciones con el delito de revelación de secretos, que no es considerado por el Código Penal Federal un delito grave, y ello permitió a los coacusados conseguir el beneficio de la suspensión provisional contra la orden de aprehensión solicitada por la PGR.

Ese proceder de acusar en falso (en extremo) fue una apuesta dirigida a producir furor patriotero y a la vez ocultar los yerros estatales que pusieron las bases de datos en la mira y a modo de los pillos que las reprodujeron y vendieron.[26]

La correcta dimensión de los daños causados a la sociedad en general y a los titulares de los datos defenestrados y las sanciones adecuadas solo podrían encontrar respuesta en una ley de protección de datos personales que aún no tenemos y que urge.

---

25 Así lo confirmó el nuevo Presidente del IFE, Dr. Luis Carlos Ugalde, quien fue interrogado en el mes de mayo del 2004 por la FEPADE para el sólo dato de corroborar que de acuerdo con los registros internos del IFE se hubiera asentado la justificación del Consejo del organismo electoral –en 1999- de autorizar el traslado de dichas bases de datos al Registro Nacional de Población y que ante lo sucedido en mayo del 2003 se canceló el convenio de colaboración del IFE con el Registro Nacional de Población.

26 La Constitución Mexicana establece en su artículo 22 el merecimiento de la pena de muerte: al traidor a la patria, según la Fiscalía Especial de los Delitos Electorales de la PGR a los responsables del caso se les fincará la culpa que tiene el que "...Tenga, en tiempos de paz o de guerra, relación o inteligencia con persona, grupo o gobierno extranjero o le de instrucciones, información o consejos, con objeto de guiar a una posible invasión del territorio nacional o alterar la paz interior.." (Código Penal, artículo 123, fracción VI)

Sin duda se extrajo información oficial confidencial pero la finalidad que movió a los participantes de los hechos delictivos no fue la de propiciar una invasión al territorio nacional, ni la de propiciar la alteración de la paz interior (es vergonzante que el caso apenas se ha difundido y lejos está de haber causado zozobra en la población) lo fines del crimen fueron estrictamente económicos y mercenarios.

III.- LOS NUEVOS REGISTROS PÚBLICOS Y PRIVADOS (LAS SI'S)[27]

En los últimos años se han aprobado leyes que crean nuevas bases de datos personales[28] que se suman a los históricos registros civiles y de propiedad. Los nuevos archivos públicos almacenan datos personales sobre antecedentes penales, carcelarios, historia escolar o educativa, hospitales y clínicas, beneficiarios de programas gubernamentales de muy diversa naturaleza.

Los registros de historial crediticio (burós de crédito),[29] han desarrollado un mecanismo de acceso al crédito en el sector del comercio, pero sin las garantías personales. El acceso y disponibilidad del historial de pago como condicionante del otorgamiento del crédito benefició a los que tienen como único respaldo el que se acredite su prestigio de pagador confiable.[30]

Empero, esos registros son frecuentemente amenazantes de los derechos de privacidad e intimidad, toda vez que son una fuente incesante de discriminación de corte laboral en medio de la desregulación. Y a la vez producen la unilateral indefensión de quienes tienen malas referencias de crédito que son incluidos en el buró sin notificación que permita al afectado impugnar esa situación de especial sujeción que puede ser o no enteramente cierta, pero inevitablemente riesgosa, porque representa un estigma a la calidad "moral" de ser un confiable sujeto de crédito y que en la actualidad se ha convertido en paralelo en un certificado de buena o mala conducta del campo del credito al de la actitud laboral que observarán quienes tengan buena o mala referencia crediticia.

Si bien en Latinoamérica han aflorado leyes de Datos Personales y *Habeas data*, las que intentan resolver las lagunas de previsión especializada para regular la actividad de algunos de estos burós de credito o de otros registros en proliferación. Destacan los casos de Paraguay,[31] México (con alguna legislación parcial),[32] Panamá ,[33] y Chile [34] señales promisiorias de un mejor porvenir.

---

27 Las Sociedades de Información.

28 Ley de Creación del Registro Nacional de Donantes de Células Progenitoras Hematopoyéticas, por Ley 25.392 de Argentina; Ley 6.879 de la Provincia de Mendoza (Argentina) sobre el Registro de Deudores Alimentarios Morosos; Ley Reformatoria a la Ley de Discapacidades de Ecuador con fundamento en el artículo 14 sobre el Registro Nacional de Discapacidades, Ley sobre Discapacidades del 4 de febrero de 1994, ver artículos 51 y 52; Proyecto de Ley en Uruguay por el que se crea un padrón especial para la inscripción cívica de aquellas personas con discapacidades físicas que así lo requieran; Ley de Transfusión y Bancos de Sangre artículo 44 de la Constitución de Venezuela; DNA Identification Act (sections 39 & 40) de Trinidad & Tobago, entre otras en proceso legislativa en tramite.

29 En algunos países los antecedentes crediticios son registrados por el Estado, por ejemplo en Argentina quienes libran cheques sin fondo son registrados por el Banco Central y en El Salvador existe una base de antecedentes crediticios administrada por la Superintendencia del Sistema Financiero.

30 Rafael del Villar, Alejandro Díaz de León y Johanna Gil Hubert, Regulación de Protección de Datos y de Sociedades de Información: Una Comparación de Países Seleccionados de América Latina, los Estados Unidos, Canadá y la Unión Europea, Banco de México, Documentos de Investigación 2001-7.

31 www.ulpiano.com/habeasdaata_paraguay_Ley.htm

32 www.condusef.gob.mx/informacion_sobre/buro_credito/leyregularlassociedades.htm

33 www.legalinfo-panama.com/legislacion/00297.pdf

34 http://lac.derechos.apc.org/legislacion/completo.shtml?x=8540

a) Datos personales: una expresión abierta y por ende peligrosa.

Al hablar de datos estaremos siempre refiriendo alguna clase de almacenamiento y difusión. Toda persona está permanentemente entregando datos de su vida privada, en algunos casos puede controlar esa comunicación y evitar que otros reciban esos datos, pero el proceso tiene sus límites pues al paso del tiempo, esos datos se quedan por ahí guardados y si no son protegidos por tener el rango de datos íntimos o sensibles pueden caer en las manos de quienes por malicia o ruindad puedan extraerlos para filtrarlos con el objetivo de dañar a sus titulares o de corresponder con ellos a las recompensas ofrecidas por tales datos.

El nombre de alguien informa sobre el sexo de quien lo lleva, el apellido revela toda una historia familiar o un origen, -señala Carlos G. Gregorio- *e incluso aquellos apellidos que han sido traducidos, fonetizados o modificados por los errores de trascripción de los registros civiles estarían mostrando además datos migratorios.* [Y Continua] *...También si un apellido es frecuente o raro estaría marcando una vulnerabilidad diferencial para los procesos de búsqueda e identificación, pues una forma de conservar la intimidad es también caer dentro de la saturación de una búsqueda.*[35]

Así las leyes que restringen o facilitan los cambios de nombres o apellidos pueden limitar o facilitar la intimidad.[36] La tendencia en la Europa unificada y en parte seguida en los países de latinoamerica es la de complicar o restringir el cambio de apellidos, mientras que en los EE.UU. es un procedimiento sencillo y hasta basado en fundamentos eminentemente subjetivos..

No existe una solución de carácter general para balancear libertad de expresión con derechos de intimidad y privacidad. Pero no es ésta la principal fuente de problemas sino la creciente tendencia a generar bases de datos.

Las más generalizadas son los buró de crédito, que son utilizadas para determinar si una persona ha fallado en el pasado en algún pago. El segundo gran conflicto es con los registros públicos (entendido como aquellos que se generan en alguna institución pública) que contienen datos personales y particularmente aquellos que contienen datos sensibles. Entre éstos los más delicados son los registros judiciales, ya que contienen información personal relacionada con conflictos entre personas que son confiados al sistema de administración de justicia para obtener una solución. En algunos países el expediente judicial es público, en otros es reservado, pero no existe duda que una sentencia judicial que ha causado estado es un documento público. Sin embargo la difusión indiscriminada de sentencias judiciales y la capacidad de un motor de búsqueda en Internet pueden llegar a un nivel de exposición de los datos personales desproporcionado con la finalidad de difundir la jurisprudencia.

---

35 Por ejemplo, una búsqueda por los nombres "Juan Pérez" produciría tantos resultados que haría prácticamente imposible cualquier proceso de identificación, por el contrario nombres originales o apellidos raros no pasarían inadvertidos. También los apellidos que tienen significado en un lenguaje nacional son menos vulnerables que aquellos que no son palabras de uso corriente.

36 En Chile la ley 17.344 permite el cambio de nombre y apellido una sola vez en la vida justificando menoscabo moral o uso continuado de otro nombre. Contrariamente otras legislaciones, en la Argentina por ejemplo, es muchísimo más restrictiva y en muy pocos casos es autorizado un cambio de nombre o apellido. Si bien en Chile la reforma legislativa se fundamentó en el derecho de las personas de reflejar en sus apellidos su pertenencia étnica, los resultados prácticos fueron que muchos mapuches cambiaron sus apellidos por apellidos españoles aduciendo que sus apellidos originales eran motivo de discriminación, ver: María Cristina Millaray Llanquileo Romero, 'Un análisis de los cambios de nombres en sujetos mapuches, 1970 a 1990', 27 Revista Proposiciones, (1996) 148-160, Santiago de Chile.

Dentro del compendio de datos personales existe un segmento de datos "sensibles"o íntimos que son los que reclaman la mayor protección posible.[37]

El resto de los datos personales son prácticamente transferibles para fines del mercado sin restricciones importantes cuando se tratan en abstracto, salvo que se individualicen supuesto que reclama mediar la autorización (consentimiento) de los titulares de tales datos.[38]

No se consideran datos personales de carácter sensible, los hábitos personales que refieran hábitos de consumo de bienes y servicios siempre que dichos datos no revelen directa o indirectamente algún dato sensible del titular.

La expresión *datos personales* es omnicomprensiva, y consiste en la información de cualquier tipo, referida a personas físicas o morales (de existencia ideal) determinadas o determinables.

Las aproximaciones legislativas (iniciativas legislativas) en México se concentran en el reconocimiento del derecho a la protección de los datos personales de las personas físicas ignorando o excluyendo deliberadamente[39] a las personas morales.[40]

Los principios que han influenciado la normación de la protección de datos personales son:

Limitación de la finalidad; calidad y proporcionalidad de los datos; información de los afectados; seguridad y deber de secreto; derechos de acceso, corrección y supresión; restricciones a transferencias ulteriores; reglas especiales para datos sensibles; derechos de exclusión en casos de *marketing;* decisiones individuales automatizadas y existencia de una autoridad de protección de datos.

b) Algunas reflexiones comparatistas en el hemisferio americano.

En el hemisferio americano se concentra justamente en los extremos de un lado Canadá y los Estados Unidos de Norte América y del otro Chile y la Argentina. Con el muy aleccionador caso del Perú, que se convierte en una realidad legislativa de gran entidad aunque probablemente por encima de la realidad de un país que ahora atraviesa enormes dificultades para llevar a buen puerto una transición a la democracia libre de amenazas.[41]

A pesar de ser Canadá, Chile y Argentina las únicos países con una legislación general para la protección de datos personales, en cambio los Estados Unidos y el Perú cuentan con una ley general que regula las sociedades de información. Sin embargo es

---

37 Datos "sensibles" son datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o política o información referente a la salud o a la vida sexual.

38 Titulares de los datos personales, toda persona, física o moral (con domicilio legal) que cuyos datos sean objeto de algún tratamiento.

39 La supresión de las personas morales como sujetos de la regulación de una ley de datos personales y de la intención de crear una agencia estatal para la protección integral de los datos personales fue resultante de la negociación del PAN para aprobar en el Senado el Proyecto Antonio García Torres.

40 Cuestión que ocurre tanto en el proyecto –convertido en iniciativa de ley- del Senador Juan Antonio García Torres como en el Banco de México.

41 Cfr el excelente estudio de Del Villar Rafael, Diaz de Leon Alejandro y Gil Hubert Johana, "Documento No 2001-7 Regulación de Protección de Datos y de Sociedades de Información: una comparación de países seleccionados de América Latina, Los Estados Unidos, Canadá y la Unión Europea", Dirección General de Investigación Económica, Banco de México, 2001.

muy diferente la experiencia que dichas regiones han alcanzado en materia de regulación de la privacidad como derecho frente al Estado y a terceros, en ello la consolidación de los sistemas de Canadá es a todas luces superior, seguida por la solución estadounidense.

Resulta particularmente interesante la concepción canadiense del asunto en tanto que ha diseñado un marco regulatorio progresivo para su sistema federal de gobierno. Canadá lleva mas de treinta años internándose en este territorio y en el afán de cerrar las brechas en el conjunto de regulaciones federales y provinciales en el año 2000 fue aprobada La *Personal Information Proteccion and Electronic Documents Act* (PIPEDA), que inició su vigencia hasta el primero de enero del 2001.

La PIPEDA es una ley general de protección de datos que es aplicable únicamente a organizaciones del sector privado. Toda vez que allá existe una ley federal que regula en exclusivo a las instituciones del sector público, el *Privacy Act* de 1983.

Y desde entonces las universidades, escuelas y hospitales quedaron para su regulación sobre la materia, en las manos de los legisladores provinciales del Canadá.

La PIPEDA vinculó desde el primer día de su vigencia a bancos, el sector de las telecomunicaciones, la teledifusión, las aerolíneas las compañías de transporte *y cualquiera otra que venda información personal dentro de las fronteras de las provincias.* Justamente ahora a partir del primero de enero del 2004, quedarán bajo la cobertura de la PIPEDA todas las compañías privadas que habían quedado fuera de su previsión inicial, como queda claro el objeto de la regulación es la actividad empresarial de comerciar con información relativa a datos personales. Allá esa cuestión se concibe como una inevitable y a la vez saludable práctica que ha alcanzado carta de naturaleza.

Y naturalmente quedan a salvo, la actividad individual de recolección de datos para fines domésticos (no comerciales: bases de datos personales) y cualquier compañía u organización que recolecte, use o transmita la información personal para propósitos periodísticos, artísticos y literarios estrictamente.

Es obligado referir que en el Canadá, los Estados Unidos y el los países de la Unión Europea la las legislaciones de comentario no se ciñen en exclusivo a la protección de la privacidad sino que intentan fomentar el comercio y el mejor funcionamiento de los mercados a través de promover el flujo de información.

1.- En el ámbito de la región sentimental (política y cultural) de America Latina

Las recientes reformas constitucionales en América Latina introdujeron la protección de los datos personales (algunas bajo la forma de *Habeas Data*), Brasil 1988[42]; Colombia 1991[43]; Paraguay 1992;[44] Perú 1993[45]; Argentina 1994[46]; y, Ecuador 1998[47]..

Es irrefutable que las leyes generales de protección de datos personales vigentes en América Latina exponen el influjo de la legislación europea, y que fueron promulgadas en Argentina 2000, Chile 1999, Panamá 2002, Brasil 1997,[48] Paraguay 2000.

42 Brasil, artículo 5° — X, XII y LXXII; artículo 105 I.

43 Colombia, artículo 15.

44 Paraguay, artículos. 33, 36 y 135.

45 Perú, artículos. 2°, 162, 203-3.

46 Argentina, artículos. 19 y 43.

47 Ecuador, artículos. 23.8; 23.13; 23.24; 94.

48. Lei que regula o direito de acceso a informações e disciplina o rito processual do habeas data.

Otros países con proyectos de ley de datos personales en espera de definción legislativa son Costa Rica, Colombia, Ecuador, México, Uruguay.[49]

Como ejemplo de la tendencia de legislar en simultáneo o inclusive previo a leyes de datos personales algunos países cuentan con leyes de transparencia y acceso a la información gubernamental, Colombia desde 1985, Perú en 2002, Panamá 2002 y México 2002.

En Chile y la Argentina[50] las leyes de protección de datos se limitan a la protección de la privacidad de los particulares, la ley chilena de Protección de Datos de Carácter Personal aprobada en 1999 y la Ley de Protección de Datos Personales de Argentina de 2000 no se manifiestan explícitamente el fin de apoyar el flujo de información, cosa que aunque parezca sofistificada, sí contempla la Ley –peruana- de Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información de 2001.

El Perú cuenta además con la Ley No 26301 que establece el proceso del *Habeas Data*[51] y que, como debe ser, regula a cualquier controlador de datos en el sector público o en las Sociedades de Información (del sector privado).

Notable es el caso de los tres países sudamericanos, que además de las leyes generales mencionadas cuentan con disposiciones particulares para el sector financiero, en consecuencia han instituido autoridades para administrar el registro de deudores, en los casos de Chile y el Perú existe la Superintendencia Bancaria y en el caso de la Argentina esa función es desempeñada por el Banco Central.[52]

2.- Los Estados Unidos de Norte América[53]

Al no contar dicho país con una ley general de protección de datos personales el complejo entramado de mas de mil ordenamientos legales de diverso nivel que contienen disposiciones referentes a la materia no ha sido un obstáculo para la evolución de una regulación, desde luego matizado o modificado en su interpretación por el resultado de las decisiones y controversias judiciales que ha motivado el funcionamiento de las Sociedades de Información (SIs).

O dicho de otra manera, en los EE.UU. la construcción del privacy right o del "right to be let alone"es realmente un cuerpo de precedentes jurisdiccionales que ha impulsado en paralelo la abundante regulación legislativa.

---

49 Algunos países han desarrollado leyes sectoriales: Venezuela 1991 Ley sobre Protección a la Privacidad de las Comunicaciones; Panamá 2002 Ley sobre el Servicio de Información sobre el Historial de Crédito; y México 2002 Ley para Regular las Sociedades de Información Crediticia.

50 Véase en extenso la excelente obra de Gonzaini, Alfredo Gonzalo, Derecho Procesal Constitucional. Hábeas Data.Protección de datos personales.Ley 25.326 y reglamentación(decreto 1558/2001 Buenos Aires, Rubinzal-Culzoni Editores, 2003. pp.432.

51 Véase en extenso la publicación que ha emitido la Defensoría del Pueblo del Perú en coedición con la United Satates Agency For International Development al respecto, El acceso a la información pública-Hábeas Data Lima, septiembre del 2003.pp.187.

52 Del Villar Rafael, Díaz de León Alejandro y Gil Hubert Johana, "Documento No 2001-7 Regulación de Protección de Datos y de Sociedades de Información... op,cit. páginas 16 y sigs.

53 Samuel Warren y Louis D. Brandeis autores de 'The Right To Privacy',55 en el que afirman:"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right to be let alone".56 Referencia que fuera escrita en 1890 y que se considera el arranque de la doctrina norteamericana sobre el tema.

La evolución del Derecho a la privacidad en los EE.UU es la de un círculo expansivo en su contenido esencia, primero ceñido a temas de sexualidad y la preservación de su intimidad, después llegó a involucrar cautelosamente temas frontera como el aborto, la oposición a recibir determinadas terapias médicas y a casos de eutanasia.

Carlos G. Gregorio proporciona en la conferencia antes referida una lista de casos que ejmplifica esa lenta pero progresiva evolución del Derecho a la privacidad en los EE.UU. En *Skinner vs. Oklahoma*[54] se deja sin efecto una ley que establecía la esterilización de ciertos criminales. En *Griswold vs. Connecticut.*[55]*Cruzan vs. Director, Missouri Department of Health*[56] (rehusar tratamiento médico), *Roe vs. Wade*[57] (aborto), y *Washington vs. Glucksberg*[58] (suicidio asistido).

La experiencia ha formado dos grandes ejes de organización legal al respecto, y de algunas leyes sectoriales que complementan el extenso marco regulatorio.

De un lado el acceso a bases de datos personales del sector público a través del *Freedom of Information Act* (FOIA) y de la otra el procesamiento de datos personales por parte de las agencias de reportes sobre consumidores (*consumer reporting agencies)* que regula el *Fair Credit Reporting Act* (FCRA).

En cuanto a las leyes sectoriales se citan las del sistema financiero, el título V del *Gramm-Leach-Bliley Act* de 1999 y el *Financial Information Privacy Protection Act* de 2000.

En síntesis el modelo norteamericano de privacidad descansa sobre la fuerza de la ley y en la capacidad de la judicatura para limitar las acciones del Estado que pudieran resultar invasiones o intrusiones en la esfera de la vida íntima de los particulares hasta antes de los tremendos atentados del 11 de septiembre del 2001, curiosamente –resulta sin embargo contradictoria a la tendencia evolutiva arriba invocada- nunca estas decisiones han enfrentado casos de terrorismo de Estado. Y mucho menos referidos a las autoridades estadounidenses dentro y fuera del territorio de los EE.UU, cuando hemos sido testigos del creciente reducccionismo del concepto de la privacidad en los hechos que se evidencia en los EE.UU, grave sería que México dejara que su ley pendiente se edificara en la visión del vecino del norte.

3.- La Unión Europea

En Europa, la protección de la intimidad parte de las medidas para evitar la inspección de personas y propiedades sin una autorización judicial, luego se expandió mediante normas penales a proteger la correspondencia como otra faceta del derecho a la vida privada. Los horrores de la segunda guerra mundial que sufrieron principalmente los europeos hizo crecer un sentimiento que cobró carta de naturaleza en la Declaración Universal de los Derechos Humanos de 1948 en la que esa vieja querella encuentra respuesta en el texto del artículo 12 del referido instrumento internacional.[59]

Dadas las circunstancias del genocidio nazi, resulta comprensible que haya sido Alemania la cuna de la primera ley de protección de datos hacia finales de 1970 en la localidad de Hesse, el impacto produjo siete años más tarde el Parlamento Federal Alemán aprobaría la ley federal de datos personales. Otras naciones europeas crearon

54 316 US 535 (1942).
55 381 US 479 (1965).
56 497 US 261 (1990).
57 410 US 113 (1973).
58 521 US 702 (1997).

normativas e instituciones de protección de los datos personales, Suecia en 1973 y Francia en 1978.

En Europa en el trance de unificación se firma en Estrasburgo en 1981 el Convenio 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal. Al interior de la Unión Europea aparece la Directiva 95/46/CE,[60] que modifica la concepción de la información personal convirtiéndola en una mercancía de protección reforzada (por tanto de gran valor) y en dicha directiva se añade la cláusula "de terceros países" que es la que define los requisitos que deben cumplir en esta materia los países que interesen relaciones comerciales con la única expresión supranacional hasta hora conocida.[61]

Naturalmente la Directiva de comento obliga a los estados miembros a tratar los datos personales mediante procedimientos lícitos y a recogerlos con fines determinados, explícitos y legítimos. Ahí es donde se convierte en un principio fundamental la exigencia de que los datos deberán ser adecuados, pertinentes y exactos, lo que en términos correlativos permite fincar el reconocimiento del derecho de acceso del titular a los datos que le son inherentes; el derecho de oposición al tratamiento y a recurrir judicialmente en caso de violación de esos derechos y la prohibición del tratamiento de datos sensibles.[62]

La tendencia actual supone el principio de uso mínimo de los datos personales y consistente con la finalidad, con preferencia por la recolección y transferencia bajo esquemas de disociación de los datos para evitar la identificación de sus titulares.

C) Las principales diferencias entre el modelo norteamericano y el europeo.

Es obligado reconocer que en términos generales la privacidad aparece en los EE.UU. como una preocupación temprana y referida a una concepción acaso más amplia que en Europa.

- La edificación del Derecho a la privacidad en Norteamerica es fundamentalmente jurisprudencial hasta que en 1974 comienzan a ser dicho fenómeno traducido en normas legislativas, a su vez la construcción del *right to privacy* por parte de la judicatura se ha traducido en un proceso de auto-regulación.[63] En

59 "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

60 Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

61 El Capitulo IV de la Directiva limita y regula la transferencia de datos a países terceros cuando "el país tercero de que se trate garantice un nivel de protección adecuado ... El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias ...". Ver, Lynn Chuang Kramer, 'Private Eyes are Watching You: consumer online privacy protection— lessons from home and abroad', 37 Texas International Law Journal (2002) 387-419 citado por Gregorio G. Carlos ..op,cit.

62 La autodeterminación informativa (el derecho a la privacidad incluye el derecho a controlar la información sobre sí mismo y la capacidad para determinar si esa información puede ser recogida y como puede ser usada) resulta de la sentencia del Tribunal Constitucional Alemán del 15 de diciembre de 1983 en relación con la ley del censo en el que prohibe al gobierno generar "un inventario de datos personales de los individuos por medio de censos gubernamentales de carácter confidencial".

63 Varias empresas y asociaciones han creado un grupo —la Online Privacy Alliance— para conducir el proceso de auto-regulación , crear un ambiente de confianza y promover la protección de la privacidad de los clientes específicamente en el comercio electrónico.

Europa gravita singularmente la experiencia histórica de los horrores del holocausto que produjo una conciencia pública a favor de la protección de datos personales con acento en los de corte sensible. Si bien cada país europeo forjó leyes de protección, el impacto comercial de las diferencias entre estas leyes motivó un proceso de homogenización que converge a una regulación unificada de protección reforzada.

- Mientras en los EE.UU el derecho a la privacidad es un derecho personal que termina con la muerte.[64] Por ejemplo, que los registros penales son susceptibles de publicidad cuando una persona muere en circunstancias extrañas con la intención de favorecer la investigación sobre las causas de su muerte. Incluso tratándose de menores de edad. En el modelo de protección de datos de la Unión Europea la intimidad y privacidad estarán siempre conectadas al honor como derecho fundamental y al de la propia imagen (aspectos de una expresión todavía mayor como el derecho al libre desarrollo de la personalidad).[65] Así podemos ver que las leyes europeas protegen la intimidad de las personas mediante cláusulas de confidencialidad post mortem[66]
- Mientras en la Europa unificada no existe jurídicamente el derecho a la invocación de la privacidad para las personas jurídicas (morales). En EE.UU. existen precedentes judiciales de proteger a las partes que así lo soliciten incluidas las corporaciones mercantiles.[67] Y lo más interesante mediante la fórmula protegida del uso de pseudónimos.[68]
- Mientras en los EE.UU. es posible perder en parte el derecho de privacidad, situación en principio inaceptable en Europa, si no existe un fundamento jamás orientado en perjuicio del bien jurídico superior. En atención a la concepción de al menos dos categorías de personas: las voluntariamente públi-

64 Ver 62A American Jurispudence 2d Privacy 25, además el derecho de privacidad es de carácter personal y la acción le cabe sólo a la persona ofendida, en Nelson vs. Maine Times (Me) 373 A2d 1221 se estableció que la privacidad de la madre no fue invadida por la publicación no autorizadas de la fotografía de su hijo. Una excepción en el common law sería la Sección 30 de la Freedom of Information Act de 1999 de Trinidad & Tobago y la Seccion 27 de la Freedom of Information Act de 1994 de Belice en las que se protege la privacidad de las personas muertas.

65 Ver Santos Cifuentes, La intimidad y el honor de los vivos y de los muertos', 162 El Derecho (1994) 404-408.

66 Ver artículos 4 y 6 de la ley.

67 493 U.S. 146 (1989). Ver Adam A. Milani, 'Doe vs. Roe: an argument for defendant anonymity when a pseudonymous plaintiff alleges a stigmatizing intentional tort', 41 Wayne Law Review (1995) 1659-712. Un aspecto similar es la protección de secretos comerciales; en México la Ley Federal de Transparencia y Acceso a la Información Pública incluye (artículo 14.) "También se considerará como información reservada: ... II. Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal;" . También en EE.UU. la Ley de Libertad de Información (FOIA) establece Sección 552. 'Información pública; ... (a) Toda división del gobierno deberá poner a disposición del público su información del modo que se estipula a continuación: ... (b) La presente Sección no se aplicará a cuestiones que fuesen o estuviesen: ... (4) secretos comerciales e información comercial o financiera obtenida de una persona que se considerase información privilegiada y confidencial;". En Europa la Directiva 95 protege sólo a las personas físicas aun cuando las leyes de Austria Dinamarca, Italia y Luxemburgo han extendido la protección a las personas morales.

68 En la ponencia de Carlos G. Gregorio se abundan ejemplos con la siguiente advertencia ...La concesión de esta protección fue inicialmente limitada casi exclusivamente a aquellos casos involucrando menores, divorcios, custodia de un hijo, manutención de los hijos o paternidad, pero en los últimos años se ha aplicado también a personas morales: en United States vs. Microsoft Corp, se permitió a tres compañías participar como amici curiae en forma anónima como "Doe Companies" y al Federal Bureau of Investigation (F.B.I.) como "John Doe Government Agency" en John Doe Agency et. al. vs. John Doe Corp.

cas[69] y las involuntariamente públicas.[70] La tradición europea sólo considera a la personas voluntariamente públicas y que éstas pierden su privacidad en función de su fama y mediando una manifestación clara de renuncia a un área determinada de su intimidad.

- Cuando en Europa se persigue la defensa de la persona a través de normas generales y uniformes que especifiquen los límites del Estado y de los particulares para el tratamiento de los datos; en Estados Unidos no hay políticas constitucionales sobre el tema, sólo existen algunas normas sectoriales, y se prefiere la revisión judicial de aquellos casos sin ignorar el implícito incentivo para la auto-regulación.[71]

IV.- EL SEMINARIO IBEROAMERICANO CELEBRADO EN ANTIGUA GUATEMALA[72] Y LAS "REGLAS DE HEREDIA" CAMINOS A SEGUIR.

a) El encuentro de Antigua

En la hermosa Ciudad de Antigua Guatemala se exploró el momento latinoamericano al respecto y se concluyó: son dos las vertientes que atraviesan el núcleo del tema, que se instala en el aparente e imposible concierto entre la persona humana y el mercado, lo que obliga un enfoque bifrontal y equilibrado, que se proponga satisfacer ambas direcciones de la inercia que dichas tendencias producen a su favor, y que desde una visión maniquea terminaría por imponer a una de estas dos premisas sobre la otra y por tanto a la extinción de soluciones a la regulación afortunada de la cuestión.

1.- La importancia económica de contar con bases de datos personales y que existan condiciones regulares del flujo o circulación de dichos datos como un factor imprescindible del mercado y la investigación científica y tecnológica.[73]

---

69 1.- Las "personas voluntariamente públicas" son aquellas que se han ubicado o expuesto ante la mirada del público por sus actividad o asumiendo un rôle prominente en instituciones o actividades de interés para el público en general. Han sido consideradas personas públicas los actores, atletas profesionales, políticos, músicos, interpretes y animadores. Se interpreta que el público posee un interés legítimo en obtener información sobre personas voluntariamente públicas, esta información puede llegar ser tan amplia que incluiría aspectos que para otras personas serían privados.

2.- Las "personas involuntariamente públicas" son aquellas que no han buscado la atención del público, pero que han sido 'noticia' como resultado de su participación o asociación con algún hecho notorio. Esta categoría incluye —por ejemplo— víctimas de delitos o accidentes, personas procesadas por delitos o personas que han realizado actos heroicos. Una persona puede tornarse involuntariamente pública —y por tanto perder parte de su privacidad— simplemente por el hecho de estar relacionada con una persona voluntariamente públicas. Explicación obtenida literalmente de la ponencia de Carlos G. Gregorio.ver nota infra.

70. Así fue definido en Carlisle vs. Fawcett Publications, Inc., 20 Cal. Rptr. 405, 414 (Cal. Ct. App. 1962).

71 Cfr Carlos G. Gregorio, ponencia.

72 Seminario Iberoamericano sobre Protección de Datos Personales, evento celebrado en Antigua Guatemala del 2 al 7 de junio del 2003, la delegación mexicana estuvo integrada por el Senador Antonio García Torres y representantes del INEGI, de Banco de México y del IFAI; se presentaron 26 ponencias y la inauguración estuvo a cargo del Dr. José Luis Piñar Mañas, Director de la Agencia Española de Protección de Datos.

73 En ese sentido Piñar Mañas, José Luis, Ponencia del Seminario Iberoamericano..." versión estenográfica de sus palabras, recogidas como documento de trabajo interno por el Dr. Eduardo Guerrero, Director de Estudios Legislativos del IFAI.

2.- El derecho ciudadano a la protección de estos datos personales, especialmente –de modo reforzado- de los datos sensibles frente al Estado o respecto de prácticas efectuadas por particulares en posesión de tales datos.[74]

Y un aspecto complementario de ambas preocupaciones y campos de actividad se refiere a la imprescindible tutela jurisdiccional de tales datos[75],normalmente mediante el *hábeas data*[76] según se hayan expuesto dichos datos a riesgos que importen la causación de daños o agravios concretos.

b) La cita de Heredia (y las reglas sobre Información judicial).

En los EE.UU. la regla general es el acceso y la publicidad, sin embargo existen reglas que restringen o prohíben el acceso a la información judicial. La reserva es absoluta en asuntos de adopción, custodia, patria potestad, salud mental y reproductiva. Complementariamente existen reglas para restringir el acceso a algunas partes del expediente, que operan a instancia de parte o de oficio.[77] También las partes pueden solicitar al juez litigar bajo pseudónimo, situación que en los últimos años ha generado un creciente número de casos judiciales en los que se autoriza el uso de pseudónimos.

Recientemente se han propuesto algunas soluciones para la difusión de información judicial;en Francia[78] y en Italia.[79]

En Canadá, en todas las provincias existe legislación que asegura el acceso público a documentos e información en manos del gobierno y, al mismo tiempo, leyes que protegen ciertos derechos de privacidad; pero el *Canadian Judicial Council* ha concluido que en términos generales el derecho de acceso tiene mayor peso que el derecho de intimidad.[80]

---

74 Ibídem.

75 El hábeas data que según Jorge García FALCONI "resguarda la intangibilidad de la reserva de la vida privada del individuo y su entorno familiar"en El juicio especial por Acción de Hábeas Data 1ª Edición, Quito, página 54.

76 El hábeas data, no es una acción procesal civil sino una garantía constitucional y obliga al funcionario que dispone la información, a presentar la información, a explicar el uso que se esta dando a dicha información y con que propósitos la entidad tiene dicha información, a su vez garantiza acceder a dicha información para en su caso exigir su actualización, corrección o supresión.

77 Ver Juan Luis González Alcántara, 'Transparencia y acceso a la información judicial', 2 Reforma Judicial — Revista Mexicana de Justicia (2003) 67-82. Recientemente se ha regresado a la práctica de los expedientes duplicados en casos sobre drogas o terrorismo (llamados "dual dockets" — uno secreto y otro para el público y la prensa) que había sido declarada inconstitucional dentro de la Primera Enmienda en U.S. vs. Valenti, 987 F 2d 708, 713 (11th Cir. 1993), ver Dan Christensen, 'Federal Court in Florida hides cases from public', Miami Daily Business Review, 12 de mayo de 2003.

78 En Francia la Recomendación 01-057 del 29 de noviembre de 2001 de la Comisión Nacional Informática y Libertades: Los editores de bases de datos de decisiones judiciales, libremente accesibles en sitios de Internet, se abstengan de hacer figurar los nombres y los domicilios de las partes y de los testigos;

Los editores de bases de datos de decisiones judiciales accesibles en Internet, mediando pago en concepto de abono, se abstengan de hacer figurar los domicilios de las partes y de los testigos.

En Italia el Codice in Materia di Protezione dei Dati Personali incluye entre las categorías de datos especiales los datos judiciales articulo 21 y el Titulo I de la Segunda Parte regula específicamente el tratamiento de datos en el ámbito judicial.

79 El Código fue aprobado el 30 de junio de 2003 y entrará en vigor el 1 de enero de 2004 sustituyendo a la ley 675/1996.

80 Ver Judges Technology Advisory Committee for the Canadian Judicial Council, 'Open Courts, Electronic Access to Court Records, and Privacy' (2003) 55pp.

Las Reglas de Heredia -sostiene Carlos G. Gregorio- parecen ser el primer instrumento que ha propuesto una definición de finalidad de la acumulación y difusión de la información judicial, con el precedente de la Recomendación Nº R(95)11 del Comité de Ministros de la Unión Europea.[81]

La clave del futuro en esta materia consiste en la adecuación de los *motores de búsqueda* a la finalidad (Regla 4) tiene un antecedente en la Ley relativa al marco jurídico de las tecnologías de la información (de Québec, Canadá), el artículo 24 dice: *"La utilización de funciones de investigación extensiva en un documento tecnológico que contiene informaciones personales y que, por una finalidad particular, se rinde público, debe ser restringida a esta finalidad."*[82]

No se puede lograr el equilibrio del derecho a saber y el del derecho a la confidencialidad de los datos de carácter personal íntimos o sensibles, si no se armoniza un sistema de protección reforzada de la información que ha de mantenerse al margen de la publicidad sin que con ello se pueda conocer como la autoridad judicial ha procedido a resolver el caso. Lo que importa es que la ciudadanía pueda acceder a la trayectoria de los casos del juzgador para medir la calidad de sus criterios sin que esa importante opción le permita enterarse involuntariamente de las características de quienes vivieron la experiencia de comentario e incluso llegar a identificarlas por rasgos como el apellido (si este es inusual en el lugar del juicio, etcétera).

Por ello los "motores de búsqueda" vienen a derribar la conocida resistencia del poder judicial en consentir la escrutabilidad (por particulares) de sus actuaciones y resoluciones cuando éstas aun no son cosa juzgada.

V.- LA PREVISIÓN NORMATIVA VIGENTE EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN MEXICO.

El derecho a la privacidad o a la intimidad personal se encuentra previsto en la correlación de los artículos 14 y 16 de la Constitución y de manera extensiva a la Carta Política conforme al artículo 133 de la Constitución, y su invocación se complementa con las disposiciones del Pacto de Derechos Civiles y Políticos y el Pacto de San José o Convención Americana de Derechos Humanos.

La inferencia del derecho a la intimidad en México es el de un derecho a la preservación de la esfera privada de cada persona y a exigir que no sea invadida dicha esfera por terceros o por el propio Estado.

La regulación infraconstitucional de los datos personales se encuentra dispersa entre distintas legislaciones, el Código Civil, la Ley de Información Estadística y

81 Autor de la ponencia de la cual la nuestra, es en no pocos aspectos un reflexión tributaria.

82 Sin embargo indirectamente la Regla de Heredia número 8 impediría una difusión indiscriminada de los datos personales de acusados o condenados por delitos, en la medida que —a partir de esa difusión— cualquier particular podría construir bases de datos de antecedentes penales. La difusión del inicio de casos penales (por ejemplo los sorteos de juzgados) parece ser la que representa mayor vulnerabilidad por dos razones: (i) las estadísticas señalan que gran parte de las acciones penales concluyen sin sentencia definitiva; y, (ii) que difundir acciones penales obligaría a difundir luego la decisión judicial que da por terminado el caso (sea una absolución, condena, sobreseimiento, o archivo), si no fuera así se estaría difundiendo información incompleta y no se ofrecería a los imputados la posibilidad de establecer con el mismo nivel de publicidad que la acción no prosperó (situación en la que se violaría la presunción de inocencia). Cfr ponencia de Carlos G. Gregorio.

Geografía (1982); Ley Federal de TAIPG (2002); Ley para regular las sociedades de información crediticia (2001); Ley Federal de Protección al Consumidor (2000).

El documento reporte de Antigua Guatemala enfatiza la necesidad de alcanzar mediante una Legislación especializada la protección de los datos personales.[83] Sin embargo, establece algunas advertencias que es preciso recoger:

1.- Existen manifiestas resistencias del sector empresarial y financiero a que la Ley limite las actividades relacionadas con el tratamiento de las bases de datos.

2.- La iniciativa del Senador García Torres reconoce el derecho del prestador de servicios a almacenar datos personales con las debidas condiciones de seguridad, lo que contradice la tendencia imperante en los países en donde existe la regulación y protección de datos personales que consiste en la determinación de la destrucción de los datos personales una vez concluida la prestación de dicho servicio.

3.- El proyecto –no enviado aún como iniciativa al Congreso- del Banco de México, plantea la figura de las Sociedades de Información. Dichas sociedades de información son personas morales que cuentan con la autorización del organismo competente para recolectar datos personales , a fin de emitir reportes de datos. La incorporación de estas Sociedades de Información se contempla como una solución intermedia a la regulación de las personas morales como sujetos obligados por una ley de la materia.

4.- La clave del consenso con los sectores del mercado mayormente identificados como afectados como prestadores de servicios de datos personales en el escenario de una ley para la materia, consiste en las condiciones de cesión de los datos personales transferibles mediante el consentimiento de sus titulares, de modo tal que dicho consentimiento y su verificación no sea un obstáculo para la gama de servicios que impulsan el comercio electrónico global entre otras transacciones vía internet. El permiso del usuario para el uso subsecuente de la información que contiene ciertos datos personales será entre otras cuestiones definitorio de la aceptación de una legislación exitosa a sus propósitos.

5.- Tendrá que despejarse la incógnita de la creación de un organismo estatal competente a título integral o la probable concurrencia competencial de algunos organismos para tales fines pero de cobertura parcial, sobre ámbitos específicos como los de los poderes de la unión y los órganos constitucionales autónomos.

83 La protección de los derechos a la dignidad, el honor y a la intimidad de las personas mediante la regulación del tratamiento automatizado de los datos personales, y la regulación del derecho de acceso a la información que corresponde a todo interesado, salvo en los casos de interés público.

El desarrollo de aplicaciones informáticas para el tratamiento de la información en áreas como la salud, el comercio y las operaciones bancarias y de valores, entre otras.

El riesgo de que los datos personales presenten errores en perjuicio del usuario. Es común encontrar archivos incompletos o con datos equivocados, sin que los interesados puedan solicitar su corrección o e incluso su eliminación.

VI.- A MODO DE CONCLUSIONES

a).- Si en el pasado los regímenes totalitarios utilizaron las bases de datos para perseguir y exterminar personas por su origen, ideología y/o religión y ahora mismo en el mundo se vislumbran nuevos y amenazantes episodios de persecución selectiva ante lo cual no existe ninguna garantía, ni siquiera en países que como los EE.UU, fuera en su día un enclave reconocido por sus avances en la protección del derecho ala privacidad, es inequívoco que se busque evitar tentaciones ajurídicas respecto a las bases de datos personales que tiene –por naturaleza de sus funciones- en posesión el Estado.

b).- La economía se impone y de todos los datos personales los usos más peligrosos de las bases de datos personales son la que se encuentran en poder del sector privado (antecedentes crediticios, laborales, arrendamientos) son archivos que las circunstancias comerciales han convertido en fuente incesante de discriminación potencial de los titulares de los datos almacenados en esos ficheros.

c).- Frente a disputa entre EE.UU. y Europa, por los dividendos comerciales derivados de una legislación compatible en materia de protección de datos personales, sin lugar a dudas el modelo de protección de datos personales que mejor se ajusta a la realidad latinoamericana, a pesar de sus democracias en precario, es el europeo.

d).- Las economías latinoamericanas necesitan agilizar el comercio con un acceso dinámico al crédito (lo que implica navegar en los sistemas de riesgo crediticio) y las restricciones presupuestales de los Estados latinoamericanos deberán intentar encontrar en Europa una fuente de reciprocidad mediante los créditos o ínsumos económicos que pueda representar la hazaña de adquirir la tecnología que implica la protección automatizada de los datos personales en poder del Estado y del control efectivo del Estado sobre el proceder de los bancos de datos personales públicos en poder del sector privado.

e).- Las leyes de acceso a la información pública gubernamental son un instrumento para el control ciudadano de la administración pública que eventualmente puede prevalecer frente al interés por la privacidad. En el caso de México esa ha sido la tendencia

f).- La protección de datos personales no puede dimensionarse como una cuestión de derechos fundamentales en exclusivo. La reciente certificación que la Unión Europea ha otorgado a la Argentina como país cuya legislación es adecuada dentro de la Directiva 95/46/CE marca una ventaja comercial significativa consecuencia de la una legislación orientada hacia la tradición europea.[84]

g).- En México, si bien la Ley Federal de Transparencia y Acceso a la Información Pública vigente a partir del 2003 contempla previsiones sobre el manejo de los datos personales en poder de los entes públicos (federales) que en el caso del *Choice Point* caso es obvio decir no se atendieron, por haber sucedido el incidente antes a la previsión legislativa, es preciso señalar que dicha legislación no introduce los procedimientos que sólo una ley especializada puede establecer para que los ciudadanos perjudicados reclamen al estado y a los particulares involucrados las indemnizaciones correspondientes.

h).- Por tanto persiste desde la Comisión Federal de Mejora Regulatoria del Gobierno Federal (COFEMER) la tesis de convertir al Instituto Federal de Acceso a la

84 Argentina es el primer país de América Latina que recibe esa certificación (Decisión 2003/490/CE del 30 de junio de 2003), que también ha sido conferida a Suiza, Hungría y a la Bailía de Guernsey. El principio de "safe harbor" es aplicado a los Estados Unidos y Canadá.

Información Pública Gubernamental (IFAI) en la agencia estatal de protección de los datos personales del nivel federal lo que sería un despropósito si antes de ello el IFAI no se hubiera convertido en un órgano constitucional autónomo para de esa manera desligarlo completamente del poder Ejecutivo Federal.[85]

i).- La iniciativa de ley (Senador Antonio García Torres) aprobada por unanimidad en el Senado es una propuesta anacrónica e insuficiente que no debe alcanzar carta de naturaleza en la Camara de Diputados.

j).- México requiere una Ley de Protección de Datos Personales que incluya el procedimiento del *Hábeas Data* , y encomendar la substanciación correspondiente, para el nivel federal a los jueces de distrito (Poder Judicial Federal) y para el nivel de autoridad local ante los tribunales del fuero común, a efecto de que ante la negativa de acceso a la información sobre datos personales en poder de las entidades públicas federales y/o locales y ante cualquier controlador de datos autorizado (las SIs) sea posible encontrar remedio a la negativa de referencia al acceso, a la rectificación y en su caso a la supresión de dichos datos por sus titulares.

k).- Es perfectamente posible -si existe sentido constitucional de Estado en la Cámara de Diputados- que del Proyecto García Torres ya aprobado en el Senado y el anteproyecto del Banco de México, se extraiga una solución ecléctica que satisfaga las exigencias de una ley razonable acorde a las exigencias del modelo europeo. La mejor debería ser una Ley General de Protección de Datos Personales, al margen, los congresos de algunas entidades federativas ya han emitido disposiciones legales incompletas (sin un procedimiento de *Hábeas Data*).

l).- Mientras tanto, no se debe ignorar que el Ombudsman federal, la Comisión Nacional de los Derechos Humanos (CNDH) y las homólogas están habilitadas –desde siempre- conforme a la Constitución (los tratados internacionales)y las leyes secundarias a intervenir en defensa del los derechos a la intimidad, al honor y a la propia imagen que sean lesionados por el Estado y sus agentes, e inclusive, si dichas afectaciones las cometieran otros particulares en la operación (translación legalizada) de algún servicio público concesionado, o que gocen de licencia o autorización estatal para la satisfacción de actividades vitales para la población que el Estado no puede efectuar directamente y aquí nos referimos muy especialmente a las de los servicios de salud (clínicas y hospitales) las educativas y otras de corte asistencial (orfanatos y asilos de ancianos, etc.).

ll.- La resolución que tome el congreso de la Unión en este trascendente asunto será un verdadero testimonio del proceso democratizador mexicano en busca de una verdadera inserción en la era de las tecnologías con corresponsabilidad social.

85 La función polivalente del IFAI. No se puede perder de vista que la naturaleza jurídica del IFAI, es la de un órgano con características de controlador externo de la Administración Pública, sin estar precisamente afuera de la misma. Lo que ofrece las modalidades de un heterocontrol (control cualitativamente independiente pero orgánicamente perteneciente al ámbito que supervisa y afecta con su labor técnica de evaluación), el Ifai, dotado de la autonomía técnica funcional y de criterio para realizar un control técnico jurídico especializado, sobre dos áreas o temáticas concretas: la directriz de la clasificación y desclasificación de la información pública y la protección de los datos personales contenida en dicha información pública que se guarda en los anaqueles y archivos de la burocracia bajo su alcance.