Diez ideas para un régimen de datos personales en clave latinoamericana

Juan Carlos UPEGUI MEJÍA

Resumen
El autor presenta en diez puntos, sugerencias complejas e innovadoras sobre la construcción de un régimen de protección de datos personales en América Latina. Upegi Mejía enmarca su análisis en la experiencia del ejercicio jurisdiccional en Colombia, Argentina y México, principalmente. En este artículo el lector encontrará argumentos para identificar el objeto a regular en el régimen de protección de datos "ideal", las confusiones y colusiones con otros derechos fundamentales, así como los subregímenes para una protección integral.

Abstract
The author presents in ten points, complex and innovating suggestions on the construction of a protection of personal data legal regime in Latin America. Upegi sets its analysis from the jurisdictional exercise in Colombia, Argentina and Mexico mainly. In this article the reader will find arguments to identify the regulation object in the "ideal" protection of data, the confusions and collusions with other fundamental rights, and the sub-regimes for an integral protection.

Derecho Comparado de la Información
julio-diciembre de 2007, pp. 133-152

1. Introducción

Para los observadores externos, y en algunos casos también para los propios, los Estados latinoamericanos viven a la zaga de los "avances" que en materia jurídica ha implicado la "sociedad de la información". Este rezago se percibe también en la producción de ideas y de categorías que busquen hacer frente a los problemas específicos que la misma supone. A la par de la celebración de encuentros internacionales sobre el tema del *habeas data* o de la protección de datos personales, y de los ejercicios de derecho comparado que se ensayan en la materia, se prolonga esa vieja dependencia teórica, conceptual e ideológica que nos ha unido a Europa y que también, hace no poco tiempo, nos hace delirar por los Estados Unidos. Esta forma de neocolonialismo parece sufrirse o gozarse con la sensación de una fatalidad. Cualquier estudio, artículo o ponencia sobre el tema de la protección jurídica de datos personales no puede soslayar la supuesta existencia incontestable de los "modelos" europeo y estadounidense, y de sus implicaciones, reglas, contenidos, etcétera. Latinoamérica, y ni qué decir de África o Asia, no existe, o existe como buen recidario de los valores agregados de esas culturas. Esta anulación nos parece, sobre todo, injusta. Lo vemos como el reflejo del desconocimiento de importantes procesos locales en la materia, y como la falta de imaginación de nuestros doctrinantes para dar respuestas consecuentes a las dinámicas y particularidades propias.

En el presente trabajo pretendemos describir diez ideas sobre un régimen de datos personales en clave latinoamericana. El régimen es ideal, pero la inspiración de tales ideas proviene de una reflexión especialmente localizada en el caso colombiano, caracterizado por la ausencia de una ley general en la materia y por una presencia activa de la jurisdicción constitucional; por los notables desarrollos adelantados

en el caso argentino, en donde la idea del *habeas data* ha conquistado lugares infranqueables; y por el interesante florecer del caso mexicano, a partir de sus novísimas reflexiones sobre la transparencia y la protección de datos personales, con la puesta en marcha de la Ley de Acceso a la Información Pública. La descripción que pretendemos no se ocupará de los detalles. Estará animada por una reflexión general sobre algunos conceptos clave, la necesidad de desmontar algunos prejuicios corrientes y la preocupación por algunas de las particularidades del caso latinoamericano.

2. Los dos conceptos clave del régimen son los datos personales, y los archivos y bases de datos sobre información personal

La importancia de estos dos conceptos es múltiple; atenderlos permite definir:

A) *El ámbito de aplicación de las normas que integran el régimen*. Para definir si un caso determinado es o no regulado por el régimen de datos personales, es indispensable verificar la concurrencia de dos elementos: los datos personales y el archivo o base de datos.

Se suele pensar, equivocadamente, que todo evento que involucra datos personales cae en el ámbito de aplicación del régimen, sobre todo cuando los medios de comunicación de masas emplean información personal. El error en estos casos es que, por lo general, no se presenta la señalada concurrencia; se olvida que es indispensable que tales eventos estén relacionados con información personal, contenida en (o extraída de) un archivo o base de datos.

B) *Los titulares de derechos y obligaciones del régimen.* La identificación de los titulares de los derechos del régimen es posible gracias a la relación que exista entre las personas y estos dos conceptos. Por regla general, sólo son titu-

lares de derechos subjetivos sobre la información personal, las personas concernidas por ella, y en algunos casos sus ascendientes o descendientes.[1] Asimismo, la definición de las obligaciones y de los distintos tipos de responsabilidad jurídica, depende de la identificación de los titulares de los archivos o bancos de datos, sobre todo cuando es posible que la titularidad y el tratamiento de la información personal recaiga en personas físicas o morales diferentes.

C) *Algunas reglas especiales del régimen.* El tipo y número de reglas que pueden ser definidas a partir de estos conceptos es abundante, por economía mencionaremos sólo tres. *Las relacionadas con las posibilidades de apropiación.* A partir de la idea de que los datos personales son aquellos que conciernen a una persona, permiten identificarla, o simplemente refieren algún evento, circunstancia o situación a ella asociada, se ha aceptado que los mismos no puedan ser objeto de apropiación, en estricto sentido, por parte de un tercero o del Estado; por el contrario, los archivos y las bases de datos personales pueden ser objeto de propiedad e incluso de propiedad intelectual.[2]

D) *Las relacionadas con la naturaleza de los datos personales*. Existen diversas clasificaciones de datos personales:

[1] A pesar de que en el caso mexicano tal idea conoce algunas excepciones, consideramos que esta situación no desvirtúa el postulado. En efecto, a partir de la Ley Federal de Transparencia y de Acceso a la Información Pública Gubernamental de la República Mexicana del año 2002 (en adelante LFTAIPG), es posible el ejercicio del derecho de acceso (derecho a la información) por parte de terceros, sobre algunos de los datos personales de los servidores públicos.

[2] Es importante resaltar la diferencia entre la información que conforma la base de datos y la estructuración de la base de datos en función de la información personal. Aquélla no puede ser objeto de derechos patrimoniales, ésta sí, en la medida en que incorpora labor o ingenio. Este problema es abordado por Parra Trujillo, Eduardo de la, "El derecho *sui generis* sobre las bases de datos en México y la Unión Europea", *Derecho Comparado de la Información*, México, núm. 3, enero-junio de 2004. A pesar de que el autor describe el problema desde la perspectiva de la teoría general de las bases de datos, nada obsta para aplicar tales reflexiones a las bases de datos de información personal.

confidenciales-no confidenciales, sensibles-no sensibles,[3] favorables-neutros-adversos, etcétera, cada una de ellas implica una especial reflexión normativa.

En el primer caso, la confidencialidad de los datos determina que para su revelación a terceros deba mediar el consentimiento previo del interesado;[4] en el segundo caso, la sensibilidad de los datos determina que la libertad de tratamiento esté más restringida, las exigencias de seguridad sean más altas, y la posibilidad de ser revelados sea reservada a casos excepcionalísimos;[5] y en el tercero, la información negativa determina que su tratamiento esté sometido a términos de caducidad especiales.[6]

E) *Las relacionadas con la naturaleza de la base de datos.* Hay varias clasificaciones de las bases de datos, la más común tal vez sea la de públicas-privadas, en la cual se involucran dos concepciones diferentes de un mismo fenómeno. Las de carácter público existen y operan bajo el principio de legalidad, quienes las administran no ejercen un derecho sino que realizan una competencia; en cambio, las de carácter privado operan bajo el principio de libertad regulada, quienes las administran lo hacen en ejercicio de sus derechos a la libertad económica, a la información, a la libertad de profesión y oficio, etcétera.

[3] Gozaíni, Oswaldo, Hábeas data *protección de datos personales*, Buenos Aires, Rubinzal-Culzoni, 2001, pp. 233 y ss.

[4] En los términos del apartado II del artículo 18 de la LFTAIPG de la República Mexicana.

[5] La extensión de los datos sensibles varía según distintos criterios, sin embargo, un caso paradigmático es el de la información genética. Sobre el punto *cfr.*, Arellano Méndez, Alberto, "La regulación jurídica de la información genética", *Derecho Comparado de la Información*, México, núm. 6, julio-diciembre de 2005.

[6] Como ocurre en Colombia a partir de los criterios señalados en la decisión SU-082 de 1995 de la Corte Constitucional, respecto de la información sobre incumplimientos de obligaciones dinerarias y el tratamiento de bases de datos sobre historiales crediticios: *http://www.constitucional.gov.co/corte/relatoria/radica.*

3. La necesidad de tomar distancia de los conceptos de intimidad, privacidad y confidencialidad

Uno de los principales obstáculos para un correcto entendimiento y diseño de un régimen de datos personales, es considerar que su fundamento, objeto y finalidad están estrechamente relacionados con el derecho a la intimidad, privacidad o confidencialidad. Este obstáculo tiene varias explicaciones: que el análisis sobre sus elementos participa de una concepción preinformática,[7] que en los países latinoamericanos la regulación del fenómeno nació como parte del derecho a la intimidad o ligado estrechamente a él, que se confunde la idea de datos personales con la de intimidad, etcétera. Frente a estas tres circunstancias es importante indicar que:

A) El análisis sobre los elementos del régimen debe ubicarse en el contexto de la sociedad de la información y de la revolución conceptual que ella implica. Esta revolución parte de la transformación de los criterios espaciales y temporales con los que se construyeron algunos de los conceptos clásicos del derecho.

En la actualidad, la información personal se puede acopiar, congelar en el tiempo, acumular indefinidamente, cruzar, integrar, analizar, editar y depurar; puede estar contenida en distintos soportes: tejidos orgánicos, documentos físicos, electrónicos, en imágenes, en formatos audiovisuales, etcétera. Estas posibilidades revalúan la idea espacial y temporal de los conceptos-valores de identidad, intimidad, propia imagen, honor, buen nombre, etcétera, e implican un fuerte desafío para el concepto clásico de sujeto; bajo estos presupuestos, hoy como nunca la individualidad aparece

7 Sobre esta idea, *cfr.* Lucas Murillo, Pablo, *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990.

fragmentada, escindida, multiplicada, y puede ser construida y remodelada virtualmente.[8]

B) La situación normativa de los Estados latinoamericanos, en sus orígenes, estuvo determinada por la asociación de los términos y los elementos del régimen de protección de datos personales a los contenidos del derecho a la intimidad.[9] Esta situación se ha ido transformando de manera considerable bajo la necesidad de reconocer autonomía a los derechos relacionados con la protección de datos personales y al *habeas data*. El nuevo camino es acertado pues permite: entender con claridad los fenómenos jurídicos concurrentes, evitar confusiones de otra forma insalvables, y proteger mejor los distintos intereses que concurren en las prácticas de administración de archivos y bases de datos personales.

C) La confusión de los conceptos de "datos personales" y de "intimidad" tiene varias facetas desafortunadas. La principal es común y a veces pasa inadvertida: se trata de la preeminencia del binomio público-privado, aplicado a la clasificación de la información personal. Bajo esta idea, inspirada en el influjo del derecho a la intimidad, se diluye la pretensión de un régimen propio para la información personal, y la misma resulta sometida por una percepción reductiva de los intereses jurídicos concurrentes, como si lo único que importara al respecto fuese determinar si la información personal es o no accesible por parte de terceros (pública o privada), dejando de lado una serie incontable de aspectos de la mayor relevancia.

Otros efectos de esta asimilación son, por vía de ejemplo: la propensión a desproteger aspectos importantes en el tra-

[8] Cifuentes Muñoz, Eduardo, "El *habeas data* en Colombia", *Ius et Praxis*, Talca, núm.1, año 3, 1997.

[9] Al respecto, véase Pucinelli, Óscar, *El* habeas data *en Indoiberoamérica*, Bogotá, Temis, 1999, pp. 196 y ss.

tamiento de la información personal, bajo el argumento excluyente de que si no se afecta la intimidad, la hipótesis respectiva pertenece a una esfera de libertad y, por tanto, no está sometida a ninguna limitación jurídica; la prolongación y extensión de las confusiones entre el régimen de protección de datos con otros regímenes, como los relacionados con el sigilo profesional, la inviolabilidad de los papeles privados, la reserva de la información estatal, entre otros; por último, el fortalecimiento de la creencia de que el único límite a la actividad de tratamiento de información personal está constituido por la intimidad de las personas concernidas por la información.[10]

4. El objeto de protección del régimen debe ser el correcto tratamiento de la información personal

Un presupuesto para toda regulación en la materia es que el tratamiento extendido y generalizado de información personal en archivos y bases de datos es una nota definitoria de la sociedad de la información. Su existencia apareja el

[10] Estas confusiones son frecuentes en distintos pronunciamientos de las autoridades encargadas de velar por la protección de los derechos del régimen de protección de datos en los Estados latinoamericanos. Sobre la fuerte influencia del concepto de intimidad en el caso mexicano pueden consultarse las decisiones de los recursos de revisión del IFAI. Un caso interesante es el de las decisiones sobre la clasificación de las fotografías de los servidores públicos como datos personales confidenciales. Al respecto, véase el expediente 933/05, consejero ponente: Alonso Gómez Robledo Verduzco, decidido por el pleno del IFAI el 28 de septiembre de 2005, donde se consideró que "el consentimiento para la difusión, comercialización y distribución de los datos contenidos en sistemas de datos personales consiste en que los individuos puedan decidir qué aspectos de su persona desean preservar fuera de la difusión pública, a fin de garantizar un ámbito privado para el desarrollo de la propia personalidad ajeno a injerencias externas. La difusión sin consentimiento de la imagen de cualquier persona constituye un atentado al derecho fundamental a la vida privada…". El ascendente de la intimidad sobre el concepto de información personal es una constante a lo largo de la decisión.

acrecentamiento de los riesgos para ciertos valores-intereses, pero también trae un sinnúmero de ventajas para otros. Esta doble dimensión (riegos-ventajas) supone afinar los ejercicios de regulación, no sólo para evitar algunas prácticas de tratamiento de información personal, sino también para promover y fortalecer otras. En esta medida, sugerimos que el objeto de protección del régimen se concentre en definir cómo debe ser el tratamiento de la información personal. Esto presupone que: *a)* esté permitido y en ocasiones sea obligatorio tratar información personal; *b)* sea necesario definir estrategias para garantizar la corrección del tratamiento, y *c)* la corrección del tratamiento esté ligada a la satisfacción de múltiples intereses-valores, tanto de carácter individual (intimidad, identidad, tranquilidad, propia imagen, igualdad, libertad) como colectivo (acceso a servicios, equitativa distribución de bienes y cargas públicas, flujo de la riqueza, cumplimiento de las obligaciones tributarias, etcétera).

5. No debe confundirse el objeto del régimen, que es el correcto tratamiento de la información, con la multiplicidad de valores que dependen de dicho tratamiento

La consideración de la información (de todo tipo) como un elemento estructurante de la "sociedad de la información" merece un tratamiento consecuente. La ubicuidad de la misma, su calidad de herramienta imprescindible, sus riesgos e innegables beneficios, obligan a replantear la inspiración clásica y sectorizada de las regulaciones jurídicas. La información personal no escapa a estas nuevas circunstancias, su administración está presente en diversos sectores de la actividad humana, en los planos público y privado, de manera nacional y transnacional. Esta suerte de condición

medular de la información personal impone un cambio de perspectiva para indicar el objeto protegido. Deja de ser funcional plantear la regulación para proteger derechos-valores-intereses exclusivos, localizados y particulares, como la intimidad, la identidad, la propia imagen, la igualdad, la tranquilidad, la libertad política, la libertad económica, la información, el acceso a servicios, el goce de derechos fundamentales de contenido prestacional, etcétera. No porque estos derechos-valores-intereses sean menos importantes, o porque hayan perdido preeminencia, sino porque una regulación sobre la información, en concreto sobre el tratamiento de información personal, debe ser pensada bajo la necesidad de atenderlos a todos ellos. Hacer depender el régimen de uno o dos intereses solamente, implicaría negar la realidad social del fenómeno de la administración de datos, y su carácter transversal. En esta medida, insistimos en la necesidad de pensar el régimen en función de una correcta administración de información personal, y rechazar la tendencia a pensarlo en función de alguno de los derechos-valores-intereses que se busca proteger mediante aquél, en perjuicio de los otros y de la utilidad y funcionalidad del régimen mismo.

6. La idea de la permanente colisión entre los derechos a la (o valores e intereses) intimidad y la información, incorpora un falso problema

Con el florecimiento de la justicia constitucional en América Latina, se confirman en estas tierras los ecos de las inquietudes europeas. Una de las fórmulas mágicas que nos ha llegado es la del llamado principio de proporcionalidad. Este principio (en una visión ortodoxa) es empleado para determinar el alcance de las competencias del juez constitucional frente al control de constitucionalidad de las leyes, y rechaza la idea de las llamadas "teorías internas" de los de-

rechos fundamentales. Según esto, el contenido de los derechos fundamentales se determina procedimentalmente, mediante la verificación paso por paso de los elementos del juicio de proporcionalidad. Al amparo de este esquema y de manera paralela, se perfiló también la idea de que los derechos fundamentales pueden entrar en conflicto en casos concretos, y que la solución de éstos, suponía la necesidad de un ejercicio de ponderación. El presupuesto para ello ha sido sostener que su estructura es la de los llamados principios (que se opone a la de las reglas) y cuya aplicación es imposible mediante el esquema del silogismo jurídico.

En el caso de los conflictos jurídicos sobre tratamiento de datos personales en Latinoamérica estas ideas han conocido una aparente tierra fértil: la ausencia de regulación y la concurrencia, en la mayoría de los casos, de dos derechos fundamentales: la intimidad y la información. Sostenemos que estos planteamientos son equivocados: *a)* porque el universo normativo y fáctico de la protección de datos personales no se reduce, ni en una parte considerable, a los derechos a la intimidad y a la información en su vertiente subjetiva; *b)* porque las supuestas colisiones entre estos intereses, o entre otros, lo que hacen es reflejar la ausencia de una regla adecuada sobre el punto preciso del conflicto, bajo la apariencia o el supuesto de que los dispositivos normativos tienen vocación regulatoria en cada caso; *c)* porque en presencia de una regulación suficiente sobre el tratamiento de datos personales, la idea de colisión tiende a diluirse, y *d)* porque la idea de colisión al aparejar la de ponderación, supone una idea de sacrificio o de negocio entre los contenidos de los derechos-intereses, que es ajena a los derechos fundamentales.

Consideramos que una definición de los límites de cada derecho-interés concurrente, permitiría observar el problema en sus justas dimensiones; esto se logra con un régimen

adecuado de protección de datos que indique hasta dónde llega uno y otro derecho, y qué está permitido y qué prohibido durante el tratamiento de datos personales.

7. El régimen debe estar integrado por dos subregímenes: un conjunto de derechos con vocación subjetiva y un conjunto de reglas y principios con vocación objetiva

El caso del régimen de datos personales debe estar conformado por dos subregímenes que comparten igual importancia. Por un lado, el régimen conformado por la serie de derechos de carácter subjetivo que le son reconocidos a las personas sobre su información personal; y por el otro, el conjunto de reglas y principios que informan, en todos sus aspectos y etapas, la actividad de tratamiento de información personal. Esto supone, para el primero de los casos, un reconocimiento de la importancia de que las personas concernidas por la información personal jueguen un papel activo en los procesos de administración de datos personales; en resumen: una valoración del régimen a partir de la libertad y la autonomía del sujeto.[11] Igualmente supone, para el segundo de los casos, la necesidad de complementar el sistema con el señalamiento de obligaciones jurídicas determinadas, valoradas a partir del interés general y con la inclusión de regímenes de responsabilidad diversos.

11 Esta idea tiene una fuerte familiaridad con el concepto de autodeterminación informativa de raigambre germánica. Sin embargo, consideramos que no puede reducirse ni asimilarse por completo a ella. Las ideas de libertad y de participación son elementos constitutivos importantes pero no los únicos. El *habeas data* puede ofrecer mayor riqueza por su adaptabilidad como un doble concepto sustancial y procedimental. Sobre el punto, en contra, véase Chirino Sánchez, Alfredo y otro, "El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica", *Protección de datos de carácter personal en Iberoamérica*, Valencia, Tirant lo Blanch, 2005, pp. 219-222.

La pretendida existencia de estos dos subregímenes implica que la actividad esté regulada bajo dos perspectivas diferentes pero complementarias, y que las personas cuenten con un sistema reforzado de protección. Entre los que integran el primero de los subregímenes deben figurar los derechos a: autorizar, conocer, incluir, actualizar, rectificar, disociar, asegurar, bloquear, certificar, suprimir, y demás derechos que permitan que el sujeto concernido por el dato, si lo desea, participe de manera activa durante todo el proceso de tratamiento de su información personal. Entre las reglas y los principios que integran el segundo de los subregímenes, la lista puede ser demasiado larga, incluimos aquí algunos de obligatoria observancia, sin que esto indique la negación de la importancia de los excluidos. Entre los principios deben figurar: durante el acopio, los de lealtad y legalidad; durante el tratamiento, los de calidad de la información (que incorpora los de actualidad, veracidad, comples y pertinencia), finalidad, seguridad, circulación restringida y temporalidad; y durante su cesión o transmisión, los de notificación, uso conforme a los fines y responsabilidades compartidas.[12]

12 La literatura sobre los "principios" es inabarcable. La recepción de los mismos por los ordenamientos jurídicos latinoamericanos es particular. En el caso mexicano ha sido invaluable el rol del IFAI, entidad que por vía administrativa los incluyó en sus "lineamientos para la protección de datos personales", publicados en el *Diario Oficial* del 30 de septiembre de 2005, *http://www.ifai.org.mx/transparencia/lineamientos_protdaper.pdf*. En el caso colombiano ha sido central el rol de la Corte Constitucional, como se puede apreciar en varias de sus decisiones; en especial la Sentencia T-729 de 2002 del 5 de septiembre de 2002, en la cual se sistematiza la jurisprudencia y se enlistan algunos de los principios que informan la actividad de administración de datos personales, *http://www.constitucional.gov.co/corte/relatoria/radicador*. En ambos, casos no existe todavía una ley general en la materia. Por último, en el caso argentino están incluidos en el articulado de la Ley 25.326, del 4 de octubre de 2000.

8. Los subregímenes pueden ser llamados de varias formas, proponemos que el primero se llame "*habeas data*" y el segundo "tratamiento de datos personales"

Una de las notas definitorias del caso latinoamericano es el caos terminológico. Esto se explica por varias razones: en primer lugar, por una recepción inorgánica de las categorías del régimen, diseñadas y nominadas por las culturas jurídicas foráneas, en especial las europeas y la estadounidense; y en segundo lugar, por una suerte de creatividad mestiza, característica de nuestro ser cultural, que nos ha conducido a la hipóstasis de elementos propios y extraños. En ese desfile de nombres hay algunos que pueden localizarse bien, como el de la "autodeterminación informativa" (que fue pensada primero en alemán); o el barbarismo ahora aceptado oficialmente de la "privacidad" (que fue pensado primero en inglés).

El del *habeas data* es más esquivo, su doble composición en latín lo salva de una identificación cultural por la lengua, y su uso extendido y generalizado en Latinoamérica, lo hace quizá una apropiación cultural legítima. Por último, el de "protección de datos" es un producto redundante del refinamiento de los términos y que nos ha llegado hace pocos años en castellano, proveniente de la comunidad europea. Ahora bien, sobre el punto de la nominación tarde o temprano habrá un acuerdo entre los Estados latinoamericanos, si es que no terminamos antes sometidos por las "maravillas" conceptuales probadas en otras tierras. Mientras una u otra alternativa se realiza, proponemos que el primer subrégimen, el de las facultades subjetivas sea denominado "*habeas data*". Dos razones para ello: su carácter mestizo y su extendida aceptación en los ordenamientos latinoamerica-

nos.[13] Asimismo, proponemos que el segundo subrégimen, el de las obligaciones objetivas, sea denominado "tratamiento de datos personales". Dos razones para ello: claridad, en la medida en que permite identificar qué es lo que se regula, y pertinencia, pues comprende de manera íntegra el objeto de regulación; no es equívoco y tampoco es limitado.

9. La titularidad de los derechos se predica de los particulares, sean personas físicas o morales. La obligatoriedad de los principios y de las reglas se predica del Estado y de los particulares

Otro de los elementos clave del régimen está relacionado con los sujetos. La pretensión de generalidad que debe inspirarlo implica también volcar la atención sobre todos los sujetos que tienen vocación de partícipes en los procesos de tratamiento de datos. En primer lugar, hay que insistir en la importancia de reconocer que los derechos del primero de los subregímenes deben ser reconocidos ampliamente, tanto a las personas físicas como a las morales. En el caso de aquéllas sin ninguna distinción, como lo impone la civilidad del Sistema Interamericano de los Derechos Humanos; en el de estas últimas, por una consideración también estructural de la sociedad de la información: la participación activa en los procesos de tratamiento de datos es necesaria para la existencia, desarrollo y buen funcionamiento de la persona moral; de otro lado, el fundamento de tal reconocimiento no desciende hasta las reflexiones sobre la necesidad de garantizar intimidad, libertad e identidad, pues ya vimos que

13 Esta aceptación tiene también sus particularidades, la más significativa es que la figura ha sido concebida como una acción constitucional propia, que sirve de garantía específica a los diversos derechos-intereses involucrados en el tratamiento de datos personales. Así en Brasil, Argentina, Perú, Ecuador, Panamá, Costa Rica y Colombia.

éstos son derechos-valores-intereses importantes, pero no centrales en la definición del régimen.

En segundo lugar, las reglas del subrégimen del tratamiento de datos personales deben aplicar a toda persona que adelante una actividad socialmente relevante de administración de datos personales. En este sentido, tanto las autoridades públicas, las personas mixtas y los particulares deben estar sometidos a sus dictámenes. La razón gira nuevamente sobre una consideración de la sociedad de la información: la actividad de tratamiento de datos personales significa poder; y el poder, en los Estados constitucionales está sometido a límites jurídicos. Ello es así independientemente del tipo de relación (de hecho, precontractual, contractual, de servicios, de orden público, de soberanía) que pueda existir entre un administrador de bases de datos, y una persona cuya información personal sea (o deba ser) objeto de tratamiento.

10. La forma como se ejercen y se determinan los derechos, los deberes y las obligaciones del régimen es susceptible de tres etapas: la directa, la administrativa y la judicial

Los conflictos que se puedan presentar con ocasión de las actividades de tratamiento de datos deben resolverse en tres etapas, de las cuales al menos la segunda es prescindible. Estas etapas son, en su orden:

A) *La etapa de reclamación directa.* Que se activa con una solicitud, por parte de la persona legitimada, frente al respectivo administrador, para que adelante alguna de las conductas que integran el objeto del derecho subjetivo de *habeas data* (dar a conocer, actualizar, suprimir, disociar, etcétera); la importancia de esta etapa estriba en que permite a la persona enterarse de las prácticas de tratamiento, y

al administrador enterarse de eventuales fallas en dicho proceso y corregirlas a tiempo; favorece la composición directa de los conflictos, y evita congestión de autoridades administrativas y judiciales.

B) *La etapa administrativa.* Se trata de un trámite adelantado por una autoridad de control competente *ex officio* o a petición de parte, con el fin de establecer si un administrador de datos ha incumplido alguna de las obligaciones generales que le impone la ley; cuando esto se verifica, hay lugar a una declaración de responsabilidad de tipo administrativo, que puede variar según la naturaleza de la base de datos (pública o privada), y que puede ser de tipo pecuniario (multas) o personal (responsabilidad personal de funcionarios, privación de derechos de administrar la base de datos, amonestaciones públicas, etcétera. Hasta el momento, esta etapa es prescindible en el caso latinoamericano, aunque bajo el influjo de las regulaciones europeas, y las experiencias de Argentina y México la tendencia se está revirtiendo.

C) *La etapa de reclamación judicial.* Es la más importante de las tres etapas, y consiste en la ventilación de los conflictos entre un administrador de bases de datos y un sujeto legitimado, con el fin de que el mismo sea resuelto de manera definitiva e inapelable. Existen varios mecanismos para esto. El típico, que le ofrece la especial singularidad al régimen, es el de la acción constitucional de *habeas data*. Concebida para engendrar un procedimiento tipo amparo, no indemnizatorio, especial, informal, célere y sumario para la protección de los derechos subjetivos relacionados con el tratamiento de datos.[14]

14 Para una descripción de esta acción constitucional en el caso argentino, véase Puccinelli, Óscar *Protección de datos de carácter personal*, Buenos Aires, Astrea, 2004, pp. 513 y ss. De otra parte, en el caso colombiano la naturaleza constitucional de este instituto es debatida, pues ha sido considerado simultáneamente un derecho y una garantía en sentido propio. Al respecto, véase Remolina

Otros mecanismos varían según las particularidades de cada Estado, pero pueden contarse los de naturaleza civil, con fines indemnizatorios y reparadores, los de naturaleza penal, y otros de naturaleza constitucional para la defensa del subrégimen del tratamiento de datos, como las acciones populares o las de inconstitucionalidad contra leyes o decretos.

11. La eficacia del régimen es diferencial, en función de los dos subregímenes

En el primero, *habeas data*, el énfasis está puesto en la responsabilidad judicial constitucional; en el segundo, tratamiento de datos personales, se traslada a una responsabilidad judicial de naturaleza diversa (civil, penal, administrativa, etcétera). La definición de los dispositivos de eficacia del régimen debe pensarse en varias claves: correspondencia con los dos subregímenes, condiciones de eficacia concretas, posibilidades económicas, y cultura y tradición jurídicas de cada pueblo.

Latinoamérica ha ensayado con éxito relativo la protección de los derechos bajo la inspiración del *habeas data* como una acción, en principio individual, para la protección de derechos subjetivos, en las coordenadas de sus Constituciones en el último cuarto del siglo XX.

Esta singular tradición regional ha puesto su énfasis en una responsabilidad de tipo judicial y de naturaleza constitucional. Consideramos que esto debe mantenerse y en lo que se pueda, por supuesto, mejorarse. Por otro lado, es cierto y reconocido que este dispositivo no es suficiente, pues existen una serie de conductas que no resultan justi-

Angarita, Nelson, "Bases para la futura regulación del *habeas data* y la protección de datos personales en Colombia", *Protección de datos personales. Memorias*, Bogotá, Defensoría del Pueblo, 2004, pp. 33 y ss.

ciables por esta vía, o cuya justiciabilidad es inútil.[15] En esta medida el régimen debe ser fortalecido con nuevos dispositivos, en algunos casos, esto ha sido ensayado con buenos resultados. La preocupación se orienta a definir mecanismos para proteger el régimen del tratamiento de datos por la vía de las disposiciones que engendran obligaciones generales. Para ello hay dos caminos: el de la responsabilidad judicial, mediante la inclusión de sanciones de tipo penal y de medidas de carácter civil disuasivo, como la acción de daños disuasoria o sancionadora; y el de la responsabilidad administrativa.

En este punto Latinoamérica sufre un dilema. El "modelo" europeo se ha afianzado precisamente sobre la creación de una autoridad administrativa independiente con amplias competencias para la protección del régimen de tratamiento de datos y, además, lo exige como el mejor indicio de que los Estados ostentan un nivel de protección de datos adecuado.[16] Sin embargo, las posibilidades financieras de los

15 Por ejemplo, el problema de la venta o la cesión de bases de datos no puede resolverse por la vía del primero de los subregímenes, es necesario complementarlo con el segundo, mediante la determinación de obligaciones claras y de una férrea responsabilidad. Un caso que ilustra esta situación es el de la compra por parte de la compañía estadounidense *Choicepoint* de varias bases de datos sobre los habitantes de distintos países de Latinoamérica. Sobre la descripción del problema en el caso mexicano véase Acuña Llamas, Francisco Javier, "La protección integral de los datos de carácter personal en México: la inaplazable elección legislativa, entre el modelo norteamericano y el modelo de la Europa Unificada", *Anuario da Facultade de Dereito da Universidade da Coruña*, núm. 8, 2004.

16 Sobre el punto, en México hay varias voces a favor, por ejemplo Antonio Avelleyra considera que "Jurídicamente, la mejor opción sería contar con una autoridad nacional con características y funciones similares a las agencias nacionales de protección de datos de los Estados miembros de la Comunidad Europea, con niveles similares de protección y una agencia responsable, lo cual es un requerimiento para establecer acuerdos de internacionales cooperación". Así en "La comunicación de mensajes de datos personales en México. El predecible estado del arte: la administración pública, los desarrollos privados y los esfuerzos legislativos 2003-2004 ", *Derecho Comparado de la Información*, México, núm. 4, julio-diciembre de 2004.

Estados latinoamericanos y alguna resistencia respecto de la verdadera utilidad (costo-beneficio) de su implementación, juegan como fuertes argumentos en contra.[17] Este es un debate pendiente de la mayor importancia, de su desenvolvimiento depende la suerte de la posible emergencia de un singular "modelo" latinoamericano.

17 El caso uruguayo es revelador. Según el comentario de Alberto Brause Bereta al proyecto de ley en la materia: "Se admite que el órgano de control estará sujeto a la subordinación jerárquica del Poder Ejecutivo, circunstancia no aconsejable idealmente. El ideal, sin embargo, no es posible plasmarlo en la realidad presente en Uruguay puesto que el país no se encuentra en condiciones políticas ni económicas de crear un órgano de control independiente". Así en su artículo "La situación en Uruguay sobre protección de datos personales", *Protección de datos de carácter personal en Iberoamérica*, *op. cit.*, nota 14, p. 342.