DANIELLE ZAROR MIRALLES

IMPLEMENTACIÓN DE UN MODELO DE AUTORREGULACIÓN VOLUNTARIA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

IMPLEMENTATION OF A VOLUNTARY SELF-REGULATION MODEL RELATED TO PERSONAL DATA PROTECTION

ARTÍCULO INÉDITO DE INVESTIGACIÓN

CÓMO CITAR ESTE ARTÍCULO (CHICAGO)	Zaror Miralles, Danielle. "Implementación de un modelo de autorregulación voluntaria en materia de protección de datos personales". *Revista de Derecho Aplicado LLM UC* 3 (2019). doi: 10.7764/rda.0.3.1069
REVISTA DE DERECHO APLICADO LLM UC	Número 3 Julio 2019 ISSN: 2452-4344
	Recepción: 4 de abril, 2019 Aceptación: 8 de julio, 2019

Resumen

El presente ensayo propone una serie de acciones preparatorias a la espera de la dictación del nuevo marco regulatorio chileno en materia de protección de datos personales. Como la regulación vigente resulta insuficiente, se hace necesario tomar decisiones a nivel directivo frente a otras variables regulatorias que se ciernen sobre la gestión de una determinada organización. En efecto, la entrada en vigencia del Reglamento Europeo de Protección de Datos Personales (conocido como GDPR, por sus siglas en inglés) con su alcance global, el alto grado de automatización y digitalización de los procesos y la muy próxima aprobación de un moderno marco regulatorio en la materia, hacen necesario que se realicen esfuerzos preparatorios, en modalidad de autorregulación voluntaria, para favorecer una transición operativa que asegure el cumplimiento gradual y efectivo de las nuevas reglas.

Palabras clave: Protección de datos personales, autorregulación, GDPR, privacidad

Abstract

This essay proposes a series of preparatory actions pending the issuance of the new Chilean regulatory framework for the protection of personal data. As current regulation is insufficient, it makes necessary to take decisions at the managerial level to face others regulatory variables that hover over the management of a specific organization. Indeed, the get in force of the General Data Protection Regulation (GDPR) and its global scope, the high degree of automation and digitalization of processes and the forthcoming approval of a modern regulatory framework on the subject make it necessary to make preparatory efforts, of voluntary self-regulation, to favor an operational transition that ensures the gradual and effective compliance with the new rules.

Keywords: Personal data protection, self-regulation, GDPR, privacy

Danielle Zaror Miralles

Universidad de Chile
Estudiante de Doctorado en Derecho
Santiago, Chile
dzaror@ug.uchile.cl

Danielle Zaror Miralles es abogada de la Universidad de Concepción, Magíster en Derecho Económico de la Universidad de Chile y Doctoranda en Derecho de la Universidad de Chile. Profesora del Diplomado en Protección de Datos Personales de la Facultad de Derecho de la Pontificia Universidad Católica de Chile.

Universidad de Chile
PhD in Law Student
Santiago, Chile
dzaror@ug.uchile.cl

Danielle Zaror Miralles is a lawyer from Universidad de Concepción, Master of Economic Law from Universidad de Chile and PhD in Law student at Universidad de Chile. Professor of the Diploma in Personal Data Protection at School of Law, Pontificia Universidad Católica de Chile.

1. Consideraciones preliminares

El presente artículo encuentra su motivación en el Diplomado sobre Protección de Datos Personales en que he tenido la oportunidad de participar como docente, y que fue realizado durante el segundo semestre del año 2018 y el primer semestre del 2019, en la Escuela de Graduados de la Facultad de Derecho de la Universidad Católica de Chile.

El objetivo del programa ha sido ofrecer un set de herramientas teóricas y prácticas sobre los principales aspectos de la regulación en materia de protección de datos, su origen y lo determinante que resulta el entorno tecnológico para la formación continua de abogados que se desempeñan en el sector público y privado, y que se relacionan con estos mismos temas.

Una parte importante del curso fue destinada a realizar un análisis de los orígenes y evolución de los hitos que dieron lugar a este derecho, hasta su consagración como garantía constitucional en Chile, así como también una serie de tratamientos específicos.

En efecto, Chile fue el primer país de América Latina en promulgar una ley de protección de datos personales el año 1999. Sin embargo, este cuerpo normativo no pudo tener una implementación idónea por carecer de una normatividad completa y, sobre todo, por no contar con una agencia que proporcionara el *enforcement* que sus normas necesitaban. La consagración de acciones civiles, las que resultan onerosas y de largo aliento, no han permitido cimentar una jurisprudencia robusta que, por esa vía, haya ido completando los vacíos. Hoy, en el panorama latinoamericano, Chile es de los países más atrasados en la materia.[1]

En la parte final del curso realizamos una serie de ejercicios prácticos con problemas reales que visibilizaron ciertas realidades que desafiaban el ejercicio de la profesión, pues es precisamente la aplicación de las normas vigentes (y sobre todo la falta de ellas) la que ha revelado un panorama que demanda de los profesionales del derecho una actitud creativa y pro activa que es, ciertamente, la que motiva la redacción de esta propuesta doctrinaria.

2. Dificultades para la implementación y aplicación de las reglas en materia de protección de datos personales

El contexto que rodea la implementación y aplicación de las reglas de protección de datos personales tiene dificultades bien particulares. En primer lugar, Chile cuenta con una regulación en la materia desde el año 1999 lo que no necesariamente significa que ésta sea suficiente o dé respuesta a las principales diatribas a las que hoy nos enfrenta este tema. Es más, buena parte de la doctrina[2] cree que esta norma nunca respondió acertadamente

1 Por el contrario, dentro de los países con regulaciones más actualizadas se encuentran Colombia, México y más recientemente Brasil.

a los desafíos que tenía que, en su época, eran básicamente hacer frente a la creciente ola de automatización, esto es, a un tratamiento que suponía «almacenamiento y operaciones lógicas o aritméticas, o de ambas, su modificación, borrado, recuperación o difusión»[3].

En segundo lugar, la falta de una agencia de protección de datos ha hecho que el tema sea resuelto por tribunales ordinarios, lo que ha dado como resultado una escasa y contradictoria jurisprudencia[4].

En tercer lugar, el anuncio de una nueva regulación en la materia[5], que ha tenido en vilo a la comunidad jurídica por lo menos desde el año 2008 y que no ha podido concretarse en una legislación idónea, ha obligado a ciertas organizaciones a tomar decisiones corporativas, incluso más allá de la regulación vigente, en orden a asegurar cierta legitimidad en los tratamientos de la información personal que realizan, más que para prepararse frente a la nueva legislación, para cumplir los estándares que ya en materia contractual se hacen exigibles (muchas veces promovidos por las organizaciones internaciones a las que adscriben).

En cuarto lugar, la dictación en la Unión Europea del Reglamento General de Protección de Datos Personales (GDPR), cuya entrada en vigencia se produjo luego de una vacancia de dos años, en mayo de 2018 y cuyo alcance ha tenido un impacto global[6], principalmente por las adecuaciones que muchas compañías transnacionales han debido realizar en su operación.

Por último, la aprobación en Chile de la reforma constitucional que modifica el art. 4º del art. 19º de la Constitución y que reconoce la protección de los datos personales y que se encuentra vigente desde junio de 2018, ha obligado a muchas organizaciones a lidiar

---

2 Cf. Manuel Vergara Rojas, "Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales", *Revista Chilena de Derecho y Tecnología* vol. 6, n° 2 [online] (2017): 135-152; Daniel Álvarez, "Acceso A La Información Pública y Protección De Datos Personales: ¿Puede El Consejo Para la Transparencia Ser la Autoridad de Control en Materia de Protección De Datos?", *Revista de Derecho Universidad Católica del Norte* vol. 23, n° 1 (2016): 51-79; Danielle Zaror, "La discusión legislativa en Chile sobre tratamiento de datos personales: Un vistazo a los últimos años". *Revista Eurolac*, nº 83 año 17. Santiago. CELARE (2011).

3 Rafael Velásquez, *Protección jurídica de los datos personales automatizados*, (Madrid: Constitución y Leyes S.A., 1993), 96.

4 Por ejemplo, en materia de aplicación de la ley 19.628 a personas jurídicas roles 961-2018, 27.889-2017, 37.301-2017.

5 Cf. *Boletín* 11.144-07.

6 Bendiek y Magnus Römer, "Externalizing Europe. The global effects of European data protection", *Digital Police, Regulation and Governance*, vol. 21 n° 1 (2019): 32-43.

con la protección de un derecho fundamental muy poco conocido por los titulares y por aquellos que deben ser sus garantes.

El contexto recién descrito, con todas esas variables concomitantes, sin duda representa una tarea que demanda de los profesionales del derecho mucho criterio y creatividad, dependiendo del ámbito en que cada uno se desempeñe. Unido a lo anterior está el hecho de que estas materias están fuertemente vinculadas con el escenario tecnológico, y este entorno es quizás uno de los más dinámicos en los que se puede experimentar.

3. Aspectos relevantes sobre la autorregulación

Existe considerable literatura disponible sobre la autorregulación, sus orígenes, sus objetivos, sus integrantes y su mejor concepto. No es este artículo el adecuado para abordarla en su integridad. Sin perjuicio de eso y en beneficio de este mismo trabajo, valga la pena explicar algunos aspectos generales sobre ella.

Tradicionalmente, algunas opiniones desde la Economía explicaban a la autorregulación como una reacción, casi como un opuesto a la regulación; la primera con límites (de responsabilidad) bien definidos para el sector privado y la segunda con un campo de acción sólo referido al Estado. Sin embargo, estas posiciones han sido desafiadas con el paso de los años, principalmente desde el Derecho y han derivado en espacios mucho más difusos de interacción; sin ir más lejos, la mayoría de las veces la organización privada que se autorregula lo hace para alcanzar dimensiones o fines públicos que son al menos compartidos desde el propio Estado.

Por esa razón es que no sorprende que las organizaciones privadas se autorregulen, en realidad, se estima que no hay ninguna novedad en esa práctica. En efecto, se puede entender que la autorregulación no es otra cosa que la puesta en práctica o manifestación de la autonomía de la voluntad, en tanto se expresa para generar un determinado contenido normativo y deslindar con mayor claridad las responsabilidades del o los involucrados en el acuerdo.

A través de la autorregulación siempre «se pretende mejorar la participación y la responsabilidad de los particulares en el cumplimiento de ciertos objetivos públicos, garantizando eficacia y coherencia para la legislación»[7], de manera que estamos frente a una particular materialización de un principio de responsabilidad general.

Pero lo que resulta innovador y que sí genera trascendencia, es que la autorregulación

[7] Maria Mercè Darnaculleta, "La Autorregulación y sus Fórmulas como Instrumentos de Regulación de la Economía", *Revista General de Derecho Administrativo,* nº 20 (2009), https://dialnet.unirioja.es/servlet/articulo?codigo=2941169.

sea promovida desde el sector público. De hecho, muchas organizaciones internacionales centran parte importante de su trabajo en materializar estos objetivos a través de la adopción de marcos de trabajo conocidos como prácticas de *Good Governance*.

Estas dinámicas dan buena cuenta de que la autorregulación también afianzó su influencia al ligarse fuertemente al fenómeno de la globalización lo que, en efecto, permite vislumbrar que gran parte de los mercados que se autorregulan son aquellos más fuertemente insertos en el contexto global (banca, seguros, energía, telecomunicaciones, tecnología, etc.).

Los sujetos y los escenarios en que estos actores se desenvuelven tienen un espectro amplio y cuyos efectos pueden ser más o menos vinculantes. Así, por ejemplo, a propósito de esta idea de espectro, José Esteve señala que la autorregulación se agrupa en tres categorías: la primera integrada por actuaciones de contenido normativo con cierto grado de abstracción (normas técnicas, protocolos, códigos de conducta); la segunda integrada por acuerdos y decisiones singulares y la tercera comprendería soluciones de conflictos, fundamentalmente por vías arbitrales o de mediación.[8]

Julia Black, por su parte, señala que la autorregulación se puede manifestar de cuatro maneras en su relación con el Estado: la primera es la *mandated self-regulation* donde es el Estado quien encarga ciertas funciones de autorregulación; la segunda es la *sanctioned self-regulation* que tiene lugar cuando un colectivo se da sus propias reglas y éstas deben ser luego aprobadas por una autoridad estatal[9]; la tercera es la *coerced self-regulation* en la que una determinada organización se impone reglas a consecuencia de determinadas condiciones impuestas por el Estado que de no cumplirse pueden derivar en sanciones[10] y la *voluntary self-regulation*, donde el Estado no se involucra ni directa ni indirectamente.[11]

La autorregulación voluntaria, que es la autorregulación promovida por este artículo, es aquella que no está ordenada por la ley (porque a la fecha no tenemos una que lo disponga para efectos de la protección de datos personales), y que resulta de la organización

8 José Esteve, *Autorregulación. Génesis y efectos*, (Navarra: Ed. Aranzadi, 2002), 15.

9 Es el caso de los Códigos de Conducta regulados en el artículo 40° y siguientes del Reglamento General de Protección de Datos de la Unión Europea. Nótese que el numeral 3° del artículo 40° también hace referencia a la autorregulación voluntaria al referirse a aquellos "responsables o encargados a los que no se les aplica el presente reglamento". En este último caso, valga la salvedad que la adhesión al Código es voluntaria, pero una vez adherido para el responsable o encargado sus reglas son vinculantes.

10 Es el caso del artículo 43° N° V de la Ley Federal de protección de Datos Personales en Posesión de Particulares de México. Aquí los sujetos podrán libremente convenir esquemas de autorregulación vinculante en la materia que complemente lo dispuesto en dicha ley.

11 Julia Black, "Constitutionalising Self-Regulation", *The Modern Law Review*, n° 49 (1996).

voluntaria de una o varias entidades para adherir al cumplimiento de ciertas directrices o pautas de conductas en orden al cumplimiento de un fin determinado. Su objetivo está orientado en el sentido de establecer ciertas reglas de trabajo o desempeño que permitan elevar estándares de cumplimiento normativo, principalmente en materia de adecuación operativa y de medidas de seguridad adecuadas[12].

El esfuerzo por autorregular de manera voluntaria busca favorecer implementaciones progresivas en lugar de cambios radicales y eventualmente preconstituir prueba o atenuantes en caso de responsabilidad civil, etc.[13]

Implementar un proyecto de autorregulación voluntaria justamente busca hacer menos drástico el tránsito desde la falta o insuficiencia de regulación en la materia hasta la entrada en vigencia de la legislación contemplada en el proyecto de ley en actual discusión y que establece estándares altísimos de cumplimiento. En efecto, no se debe perder de vista que el proyecto de ley hace una referencia a la autorregulación obligatoria en materia de transferencia internacional de datos (art. 27| letra c), pero también hace una referencia a un modelo de autorregulación voluntaria, cuando regula lo que denomina "Modelo de Prevención de Infracciones" (art. 52| inciso II), al señalar que "podrán voluntariamente adoptar". En los dos casos, como resulta lógico a estas alturas, el resultado de ambas autorregulaciones resulta vinculante, sin embargo sus efectos son distintos.

En el primer caso, la autorregulación es requisito *sine qua non* para la transferencia internacional. En el segundo caso, según lo dispuesto en el art. 54° del proyecto de ley, la existencia de un modelo de prevención de infracciones.

Como se señala en el primer punto de este trabajo, lo que se pretende es ofrecer una breve guía sobre las acciones iniciales o contenido mínimo que debería seguir una asesoría jurídica o departamento legal que pretenda generar mecanismos o instrumentos de autorregulación voluntaria con efectos vinculantes en una organización, ya sea pública o privada.[14]

---

12 Una fuente muy útil para orientar los primeros pasos en esta tarea es la visita al sitio web de la Agencia Española de Protección de Datos que cuenta con varias "Guías Generales" en materia de elementos para el cumplimiento normativo, para el responsable del tratamiento de datos personales, para el análisis de riesgos, para las evaluaciones de impacto en la protección de datos personales, etc.

13 Un trabajo académico relacionado con responsabilidad civil se encuentra en la tesis de pregrado de Bárbara Parada denominado "El Régimen de Responsabilidad Civil en la Protección de Datos Personales en Chile". En opinión de la autora de la tesis la ley vigente se inclina por un régimen de responsabilidad por culpa. Págs. 74 y 140.

14 En Chile tienen cabida los modelos de autorregulación, prueba de ello es la reciente dictación de la Ley N° 21.000 sobre la Comisión del Mercado Financiero, que introdujo reglas relativas a la autorregulación de las entidades financieras que regula.

4. El diagnóstico y el tipo de organización

Como la implementación de un plan de regulación supone una modificación de las actuaciones con la meta de reducir riesgos jurídicos, resulta cardinal contar con un buen diagnóstico de la situación. Dando por supuesto que se cuenta con el respaldo de los responsables de la organización para llevar adelante este plan de autorregulación, la primera tarea que corresponde dilucidar para dar origen al diagnóstico es el tipo de organización a la que se pertenece y para facilitar esta tarea responderemos las siguientes interrogantes generales.

4.1 ¿Cuál es la naturaleza jurídica de la organización?

Si los servicios se prestan en el sector privado, lo primero es identificar el objetivo social de la persona jurídica en cuestión. De lo anterior se sigue que, en principio, se aplica el marco general vigente en materia de protección de datos personales (Ley N° 19.628). Sin embargo, si la organización es de aquellas que pertenecen a un sector regulado la respuesta debe buscarse en el marco jurídico que rige la actividad.[15] Si este es el caso y si existen reglas propias, deberá estarse a ellas, y si ellas no existen corresponderá aplicar el marco general vigente que ofrece la Ley N° 19.628.

Si la organización es de aquellas que pertenecen al sector público se debe estar al principio de legalidad y revisar la o las leyes vigentes que regulan orgánicamente las funciones y atribuciones de dicho organismo, además de su definición, esto es, para qué fue creado el organismo respectivo. Es común encontrar regulaciones orgánicas que nada expresan respecto de este tema, sobre todo las que datan de muchos años; en estos casos, se aplica de manera supletoria la Ley N° 19.628. Téngase presente que la regulación en materia de tratamiento de datos personales de los servicios públicos que contiene la ley vigente es bastante pobre. De hecho, es posible constatar cómo aquellos marcos orgánicos más recientes traen su propia regulación en materia de tratamiento de datos.[16]

Es probable que la dirección de la organización tenga declaradas una serie de misiones y visiones, reconocimientos frecuentes que, hoy por hoy, se expresan en ambos sectores. Esos aspectos son igualmente relevantes para establecer el marco de acción y en gran medida representan el punto de partida de cualquier trabajo que pretenda aplicarse transversalmente a una organización determinada.

En esta etapa es necesario además consignar que el derecho a recoger esos datos por el organismo público respectivo se encuentra, por regla general, establecido en su ley or-

15 Por ejemplo, la Ley N° 18.933 a propósito del acceso a las fichas clínicas por parte de la ISAPRES.

16 Por ejemplo, la Ley N° 20.530 del año 2011 que crea el Ministerio de Desarrollo Social establece en sus arts. 3° letra t) y 10° reglas especiales.

gánica, por lo que el estudio exhaustivo de esta norma resulta clave para el éxito de este trabajo, pues es ahí donde puede encontrarse la fuente que autoriza el tratamiento y que eventualmente puede liberar al responsable del tratamiento de datos de exhibir o contar con el consentimiento del titular de los datos[17].

4.2 ¿Cuántas bases de datos existen?

A continuación, los profesionales a cargo del trabajo diagnóstico deben hacer un listado del número de bases de datos que se posee al interior de la organización, esto es, aquellas que tienen asignadas por ley un determinado servicio público y aquellas que han creado en virtud de los servicios que venden o que prestan, tratándose de las personas jurídicas con o sin fines de lucro.

Como punto de partida hay que decir que toda organización, independiente de su naturaleza jurídica tiene, al menos, tres bases de datos, esto es, la de sus empleados[18], la de sus proveedores y la de sus clientes o beneficiarios. En el caso de los servicios públicos también ocurre que muchas veces se gestionan bases de datos que vienen establecidas en otras leyes o en glosas presupuestarias. Este último punto no debe ser olvidado, puesto que representan la fuente legal que permite y legitima ese tratamiento por parte de los servicios públicos y debe ser visibilizada en el diagnóstico.

El caso de las municipalidades parece ser de estos últimos. Su ley orgánica nada dispone sobre el tratamiento de datos personales, sin embargo, se trata de organizaciones que administran una variedad de bases de datos que encuentran su origen en otras leyes, por ejemplos, registro de licencias de conducir, bases de datos de salud municipal, de educación municipal, seguridad o video vigilancia municipal, etc.

Conocer el número exacto de bases de datos que se posee es determinante para la gestión de ellas, pues muchas veces crecen en el tiempo y no hay conciencia institucional de este incremento.

---

17 María del Mar Pérez, "Los Ficheros Públicos", *Estudios sobre administraciones públicas y protección de datos personales,* ed. Por Antonio Troncos Reigada, (Madrid: Agencia de Protección de Datos de la Comunidad de Madrid, 2006) 117-118.

18 El Código del Trabajo establece en el art. 154 (bis) "El empleador deberá mantener reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral." Al respecto se sugiere revisar el trabajo de tesis de pregrado de Paula Jaramillo y Bárbara Sabaj, "Derecho a la Protección de los Datos Personales del Trabajador". En particular se releva el hecho de que "debido a la complejidad y duración en el tiempo (la relación laboral) es una de las fuentes más prolíficas de datos", pág 48.

Con el panorama claro del número de bases existentes, es necesario que el profesional a cargo realice preguntas mucho más específicas, pues esto facilita la comprensión global del proceso en el que se está inmerso. En este sentido, es indispensable:

- Identificar la fuente legal o de negocio de la que se deriva o justifica la gestión de esa base de datos[19].
- Saber qué tan trascendental es para la operación de la organización el tratamiento de datos personales que realiza, esto puede dar luces acerca de qué tan crítico resulta este proyecto de autorregulación para el futuro.
- Visibilizar el volumen de información que tiene cada una de las bases de datos.
- Responder acerca de la existencia o no de protocolos o procedimientos u otras normas de carácter técnico existentes. Es probable que en este caso lo único presente sean prácticas, por lo que toca describirlas por más desformalizadas que ellas sean.
- Existencia de medidas de seguridad física y lógicas. Esta pregunta es distinta a la anterior por cuanto supone listar aquellos aspectos vinculados, por ejemplo, a los controles de acceso, a la capacidad tecnológica contratada por la organización, etc.
- Naturaleza de las bases de datos, esto es, si ellas son automatizadas o no. En muchos casos la situación se complejiza porque hay muchas bases de datos en archivos documentales los que deben seguir reglas y protocolos distintos. En el caso que las bases de datos estén sometidas a tratamientos de automatización, esto es, que «su almacenamiento y operaciones lógicas o aritméticas, o de ambas, su modificación, borrado, recuperación o difusión»[20], las medidas deberán acomodarse a este estándar.
- Naturaleza jurídica de los datos almacenados en las bases según lo dispuesto en el art. 2º de la Ley Nº 19.628 (si son sensibles o no, básicamente).
  Responder la pregunta anterior nos permite inmediatamente avizorar el o los riesgos asociados a dichas bases de datos, por lo que a continuación de la naturaleza jurídica del dato se debe identificar su nivel de riesgo.
  En el mismo ítem de riesgo es conveniente responder acerca de la naturaleza de éste, así por ejemplo, si es vulnerable a un acceso no autorizado, interrupciones, ataques intencionados, etc.
  Listada la naturaleza de los riesgos se debe clasificar específicamente si éste es alto, medio o bajo.

---

19 Rodrigo Gutiérrez, "Consideraciones y Recomendaciones en Materia de Tratamiento de Datos Personales por Organismos Públicos", *Chile y la Protección de Datos Personales. ¿Están en crisis nuestros derechos fundamentales?*, (Santiago: Ediciones UDP, 2009) 47-55.

20 Rafael Velásquez, *Protección jurídica de los datos personales...*, 96.

5. La planificación y el plan de autorregulación

Establecidos estos puntos perimetrales (autorización directiva, objeto social/definición legal, atribuciones, misión y visión, tipo de datos en poder de la organización y riesgos), es necesario formular una planificación destinada a la elaboración de un instrumento de autorregulación, la que debe definir varios aspectos claves para su implementación, avance y éxito.

5.1 La cobertura

El instrumento debe establecer si el plan de autorregulación abarcará sólo uno o algunos aspectos de la gestión organizacional o la abarcará en forma total (uno, varios o todos los procesos/unidades). Lo anterior determina el plazo que se asignará para el cumplimiento de los objetivos, el presupuesto destinado y también el o los equipos directivos que será necesario movilizar.

En este punto quizás la sugerencia es que la planificación destinada a implementar un plan de autorregulación comience con procesos pilotos que no abarquen toda la organización, de manera que los errores en la ejecución puedan corregirse a medida que la ejecución y ampliación en cobertura avance.

Tanto en el sector público como en el privado existen distintos dispositivos que resulta necesario conjugar para el éxito del plan. Atendida la envergadura del proyecto de autorregulación se hace necesario convocar los talentos que los distintos equipos poseen y, en este sentido, hay al menos tres grupos indispensables que forman esta fuerza de tarea: los equipos jurídicos, técnicos y directivos. A cada uno de estos equipos, que forman la capacidad institucional del plan, se les deben asignar tareas concretas, asociadas obviamente a las funciones que realizan y a plazos fatales para reportar su avance.

5.2 Los plazos

La ejecución de lo planificado puede significar en muchos casos la contratación de nuevos servicios, la elaboración de bases técnicas para la realización de licitaciones públicas, etc. En este caso, la planificación debe contemplar debidamente entre los plazos, el tiempo que este tipo de operaciones requiere. La mayoría de las veces los equipos subestiman estos eslabones del proceso de planificación, lo que repercute en la señal y ánimo de avance y en la percepción del éxito asociada al cumplimiento del proyecto dentro de los plazos.

5.3. La gestión para el cambio

La planificación también debe abordar la cesación o reemplazo de ciertas prácticas profesionales y culturales. En escenarios de cambio, incontables veces la reiterada frase “es

que siempre lo he hecho así" resulta más difícil de remover de lo que se piensa, por lo que la formación del capital humano disponible resulta un elemento crucial para que el trabajo de planificación y el plan de autorregulación en curso, sea exitoso. Convencer y persuadir a los directivos es una parte importante (se enciende el motor), sumar al resto de la organización es igual o más determinante en algunos casos, pues es este último grupo el que pondrá en práctica los cambios y será el que probablemente perdure en el tiempo, por lo que su participación es determinante para el éxito de estas medidas (es el que mueve el carro).

6. Los objetivos del plan de autorregulación

Resulta indispensable para el logro de un plan de autorregulación exitoso que el plan contenga metas en el corto, mediano y en el largo plazo y que los hitos de cada meta estén sujetos a algún tipo de métrica que permita a sus responsables exponer medios de verificación objetivos a los directivos de la organización a la que se pertenece.

Para comenzar, el plan de autorregulación debe documentar los objetivos que se busca cumplir asociados a las medidas de seguridad, así por ejemplo, si lo que se posee es una base de datos sensibles, cuya administración debe garantizar una continuidad en la prestación del servicio, el objetivo debe estar dirigido a que estos datos sean exactos, adecuados y protegidos con las máximas condiciones de seguridad que se puedan implementar en la organización a la que se pertenece, con la idea que se esté cautelando el cumplimiento de principios como calidad, finalidad, responsabilidad y seguridad de los datos.[21]

Para cumplir con estos objetivos o metas es indispensable que ellos se construyan al alero de tres pilares de seguridad básicos: la confidencialidad, la integridad y la disponibilidad del tratamiento de los datos.

- La confidencialidad se ve amenazada por las fugas, filtraciones y accesos no autorizados.
- La integridad se ve amenazada por la manipulación, corrupción y la falta de calidad de la información.
- La disponibilidad del tratamiento se ve amenazada por interrupción y discontinuidad.

21 Un ejemplo concreto y operativo es el descrito por Uriarte (2009, 37-45) donde se expone cómo las compañías de seguros generaron una plataforma para compartir información de sus asegurados a través de denominada "Sistema de Información de siniestros de seguros generales" SISGEN. La entidad estimó, el año 2000, que las condiciones del tratamiento de datos debían incrementarse y generaron un mecanismo de autorregulación centrado en la confidencialidad e integridad de la información que se compartía.

Una vez que se identifique el proceso al que pertenece la base de datos y se perfilen los objetivos que se busca alcanzar, es necesario que se listen los riesgos para cada uno de los procesos incorporados en la cobertura del plan de autorregulación. Por ejemplo, ante el riesgo o amenazas de discontinuidad o accesos no autorizados, la organización debe tener planificada y preparada una respuesta específica.

7. Las medidas de seguridad

Las medidas de seguridad pueden ser de distinta naturaleza: están las técnicas y organizativas. Ellas pueden recaer indistintamente en las bases de datos, en los establecimientos, en los equipos y, por supuesto, en las personas. El tipo de medidas, como ya lo hemos señalado, dependerá del tipo de datos, su finalidad y la disponibilidad tecnológica que ofrezca la organización.

Así las cosas y visibilizados los riesgos, es el momento de planificar las medidas de respuesta y su correlativo responsable institucional, por ejemplo, identificado que sea un acceso no autorizado a la base de datos, lo que corresponde es generar o incrementar mecanismos de control de accesos físicos y lógicos. Frente a un riesgo de pérdida o destrucción de datos, la medida de respuesta pareciera ser una actividad tendiente a la creación de mecanismos de respaldo a través de digitalización o copia de documentos claves, etc.

Como señalamos, la declaración de un objetivo general, como lo sería por ejemplo, "identificar responsables de la gestión documental", trae aparejada una serie de objetivos específicos que, en el caso del plan de autorregulación, no es otra cosa que las acciones concretas que ese profesional debe observar desde que entre en operación el instrumento que contiene el plan.

Dependiendo del tipo de medida concreta que se adopta, se sigue el nombramiento de dos figuras indispensables para los escenarios tecnológicos y legales[22] el primero es el oficial o encargado de seguridad de la información y el segundo es el oficial o encargado de protección de datos.[23]

7.1 Encargado de seguridad de la información

Es conocido como CISO por sus siglas en inglés (*Chief Information Security Office*) y su función es la de ejecutar las decisiones que recaen sobre las tecnologías de la infor-

22 Pawel Drag y Mateusz Zsymura, "Technical and Legal Aspects of Database`s Security in the Light of Implementation of General Data Protection Regulation". Praga: *CBU International Conference on Innovation in Science and Education* (2018): 1056-1062.

23 El GDPR le denomina Delegado de Protección de Datos Personales en sus artículos 37 ° y siguientes. El Proyecto de Ley chileno por su parte lo regula en el art. 52°, asignándole la misma denominación.

mación, la continuidad operacional y las medidas de seguridad físicas y lógicas de una organización. La mayoría de las veces el perfil para esta responsabilidad está asociado a profesionales del área de la ingeniería.

7.2 Encargado de protección de datos

Es conocido como DPO por sus siglas en inglés (*Data Privacy Officer*) y su rol es el de asesorar al responsable del tratamiento de los datos, es decir, al jefe de servicio o al directorio que representa a una empresa, en la creación y gestión de una estrategia que asegure el cumplimiento legal en materia de protección de datos y privacidad. Su perfil está fuertemente ligado al mundo del derecho y sus funciones suponen que posea conocimientos especializados en normativa y práctica en materia de protección de datos personales.

Este último cargo se encuentra expresamente reconocido por el Reglamento General de protección de datos en el art. 37º y 38º de su texto, donde quizás resulta relevante mencionar que el texto señala que no importa el tamaño de la organización (éste se debe nombrar siempre), si el núcleo del negocio tiene que ver con tratamiento de datos personales.

Como señalamos en párrafos anteriores, atendiendo la envergadura del plan de autorregulación, se hace necesario establecer un cronograma que permita ir controlando el logro de los objetivos técnicos y jurídicos en el corto, mediano y largo plazo, determinado por el número de etapas en que se ha planificado la implementación.

8. Documento

Una vez materializadas estas medidas se hace necesario cristalizar el trabajo en el plan de autorregulación. Este instrumento debe contener como mínimo:

- La identificación de la o las bases de datos cuyo tratamiento se realiza en la organización y la fuente legal que autoriza su tratamiento.
- Lo que se espera de los funcionarios o trabajadores, así como de los procesos o unidades que participan en el tratamiento de datos personales.
  Identificación de los responsables funcionales de cada una de las bases de datos y del personal autorizado para operar en ellas.
- Descripción de los riesgos y de las medidas de seguridad correlativas.
  Procedimientos de mitigación.

Una vez plasmado el documento que contiene el plan de autorregulación, éste debe estar sujeto a revisiones periódicas, las que deben documentarse debidamente[24].

[24] Ana Portera, *La auditoría de seguridad en la protección de datos de carácter personal*, (Madrid: Ediciones Experiencia, 2004) 121-127.

Es importante destacar que todo plan de autorregulación no debe desatender los mecanismos comunicacionales y de capacitación dentro de la organización, pues como indicamos en párrafos anteriores es aquí donde se producen efectivamente los cambios en la cultura institucional.

9. Los Códigos deónticos

Sea que lo que se autorregule constituyan procesos de tratamiento de datos o una base singular, es pertinente señalar que estos planes pueden acompañarse de la dictación de códigos de conducta corporativa en materia de tratamiento de datos.

Estos documentos recogen con frecuencia los principios asociados a una materia específica (en este caso licitud, seguridad, finalidad, responsabilidad, proporcionalidad, exactitud, etc.) y los desarrollan conceptualmente, entregando además ejemplos concretos asociados a la actividad que se realiza para ilustrar a sus funcionarios o trabajadores acerca de un determinado modo de proceder. Se trata de «un documento que plasma el deber ser»[25].

Sin perjuicio de lo anterior, es pertinente señalar que su utilidad es acotada y no impacta en la gestión de la organización de la forma que lo hace un plan de autorregulación como el propuesto. Se trata más bien de medidas que acompañan los procesos de capacitación o de formación continua. El valor de estos códigos está más bien dado por su carácter supletorio, es decir, por establecer principios atemporales que permiten ir interpretando ciertas prácticas y mostrando un camino cuando la problemática no se encuentra resuelta de manera concreta y necesita ser disipada en base a alguna orientación valórica declarada por la organización respectiva.

10. Conclusión

La propuesta formulada busca entregar luces acerca de las acciones indiciarias que debería seguir una organización que se prepara para la adopción de estándares superiores que, sin duda, serán aquellos que establezca la nueva legislación.

La preparación y tránsito progresivo hacia la próxima normativa sobre protección de datos personales tiene hoy el mejor escenario posible. El mercado entero se está adecuando y, en el caso del sector público, ya existen muchos organismos con altos grados de protección de datos personales establecidos en sus leyes orgánicas, de manera que implementar, a través de planes piloto, incrementos en medidas de seguridad y protección parece ser el más amigable camino posible. Dicho de otra manera, estamos en esa ventana de tiempo donde el ensayo puede resultar exponencialmente virtuoso y el error mínimamente dañino.

---

25 Raúl Arrieta, "Autorregulación y Protección de Datos Personales", *Uso y abuso en la protección de datos personales*, (Santiago: Expansiva, 2011), 17.

Como es posible percibir en la reflexión ofrecida, la generación de equipos interdisciplinarios es la condición *sine qua non* para lograr concreción de los planes, la madurez de los procesos y la adopción de la cultura de la protección de datos personales en todo el espectro de la organización.

Adicionalmente, no hay que perder de vista que las prácticas de autorregulación permiten adoptar modelos que adecuan lo establecido en la ley a las características específicas del tratamiento que se realiza y, en ese sentido, su complementariedad se vuelve esencial, pues logran llegar a aspectos que la regulación general no habría podido desarrollar.

Finalmente, desde la perspectiva de los titulares de derechos de protección de datos, estos mecanismos de autorregulación representan una garantía adicional de seguridad y protección frente al régimen general establecido por las leyes. ▣

Agradezco genuinamente a mis pares evaluadores por los valiosos y generosos comentarios que formularon para mejorar la estructura y contenido de este trabajo, el que se ha visto objetivamente beneficiado con ellos. Los puntos de vista vertidos, los errores y las omisiones son estrictamente mi responsabilidad.

BIBLIOGRAFÍA

- Alvarez, Daniel. "Acceso A La Información Pública y Protección De Datos Personales: ¿Puede El Consejo Para la Transparencia Ser la Autoridad de Control en Materia de Protección De Datos?". *Revista de Derecho Universidad Católica del Norte* vol. 23, n° 1 (2016): 51-79.
- Arrieta, Raúl. 2011. "Autorregulación y Protección de Datos Personales". *Uso y abuso en la protección de datos personales.* Santiago: Expansiva (2011): 7-24.
- Bendiek, Anegret y Magnus Römer. "Externalizing Europe. The global effects of European data protection". *Digital Police, Regulation and Governance,* vol. 21, n° 1 (2019): 32-43.
- Black, Julia. 1996. "Constitutionalising Self-Regulation". *The Modern Law Review*, nº 49 (1996): 24–55.
- Cerda, Alberto. *La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales.* Santiago, Chile: Universidad de Chile. Facultad de Derecho, 2003.
- Darnaculleta, María Mercè. 2009. "La Autorregulación y sus Fórmulas como Instrumentos de Regulación de la Economía". *Revista General de Derecho Administrativo*, nº 20. Iustel. Madrid (2009) https://dialnet.unirioja.es/servlet/articulo?codigo=2941169
- Drag, Pawel y Zsymura, Mateusz. "Technical and Legal Aspects of Database`s Security in the Light of Implementation of General Data Protection Regulation". Praga: CBU *International Conference on Innovation in Science and Education* (2018): 1056-1062.
- Esteve, José. *Autorregulación. Génesis y efectos.* Navarra: Ed. Aranzadi, 2002.
- Gutiérrez, Rodrigo. "Consideraciones y Recomendaciones en Materia de Tratamiento de Datos Personales por Organismos Públicos". *Chile y la protección de datos personales. ¿Están en crisis nuestros derechos fundamentales?* Santiago: Ediciones UDP (2009): 47-55.
- Jaramillo, Paula y Bárbara Sabaj. "Derecho a la Protección de los Datos Personales del Trabajador". Santiago, Chile: Universidad de Chile, Facultad de Derecho, 2003,

- Parada, Bárbara. "El Régimen de Responsabilidad Civil en la Protección de Datos Personales en Chile". Santiago, Chile: Universidad de Chile, Facultad de Derecho, 2008.
- Pérez, María del Mar. "Los Ficheros Públicos". *Estudios sobre administraciones públicas y protección de datos personales*, ed. Antonio Troncos Reigada. Madrid: Agencia de Protección de Datos de la Comunidad de Madrid (2006): 117-123.
- Portera, Ana. *La auditoría de seguridad en la protección de datos de carácter personal*. Madrid: Ediciones Experiencia, 2004.
- Uriarte, Mikel. "El tratamiento de los datos personales en la determinación del riesgo". *Chile y la protección de Datos personales. ¿Están en crisis nuestros derechos fundamentales?* Santiago: Ediciones UDP (2009): 37-45.
- Velasquez, Rafael. *Protección jurídica de los datos personales automatizados.* Madrid: Constitución y Leyes S.A., 1993.
- Vergara Rojas, Manuel. 2017. "Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales". *Revista Chilena de Derecho y Tecnología* vol. 6, n° 2 [online] (2017): 135-152.
- Zaror, Danielle. "La discusión legislativa en Chile sobre tratamiento de datos personales: Un vistazo a los últimos años". *Revista Eurolac*, nº 83 año 17. Santiago. CELARE (2011).