https://doi.org/10.18800/derechopucp.202002.005

DERECHO PUCP
N° 85, 2020
diciembre - mayo
pp. 139-174
REVISTA DE LA FACULTAD DE DERECHO

El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano

The principle of proactive responsibility: An opportunity for better compliance with the normative regarding the protection of personal data in the Latin American field

FRANCISCO JOSÉ SANTAMARÍA RAMOS*
Universidad Complutense de Madrid (España)

Resumen: El presente estudio trata de determinar si el principio de responsabilidad proactiva, establecido en el Reglamento General de Protección de Datos europeo, puede ser fácilmente transferido al ámbito latinoamericano a pesar de que la normativa latinoamericana se encuentra excesivamente fragmentada y, en todo caso, no incluye el principio de responsabilidad proactiva como uno a tener en cuenta en materia de protección de datos de carácter personal. Esta investigación es de tipo bibliográfico y se aproxima al conocimiento del tema para identificar qué se conoce y qué no sobre el objeto de estudio. Por lo tanto, se pretende realizar una sinopsis que aglutine diferentes investigaciones, informes y artículos que den cuenta del estado actual del fenómeno a investigar; no obstante, dicha revisión implica, asimismo, la realización de una valoración crítica de las investigaciones y artículos. En este sentido, comprender cada caso examinado suministra percepciones y explicaciones inestimables para la comprensión del tópico del objeto de estudio, y permite proponer estrategias que mejoren la problemática, lo cual ayuda a poner el tema en su respectivo contexto. La bibliografía ha sido seleccionada tanto por su utilidad en el presente campo de estudio como por su actualidad, buscando revisar el material bibliográfico más importante y actual posible.

Palabras clave: Era del conocimiento, protección de datos, responsabilidad proactiva, delegado de protección de datos, normas corporativas vinculantes, evaluación de impacto

Abstract: This study tries to determine whether the principle of proactive liability, established in the European General Data Protection Regulation, can be easily transferred to the Latin American sphere despite the fact that Latin American regulations are excessively fragmented and, in any case, it does not include the principle of proactive responsibility as one to be taken into account in the protection of personal data. This investigation is of a bibliographic type and it approaches to the knowledge of the subject to identify what is known and what not about the object of study. Therefore, the objective is to carry out a synopsis that brings together different investigations, reports

* Doctor en derecho. Abogado especialista en derecho informático y profesor asociado de la Universidad Complutense de Madrid, España.
Código ORCID: 0000-0002-4538-7793. Correo electrónico: fsanta02@ucm.es

and articles that account for the current state of the phenomenon under study; however, such a review also implies making a critical assessment of the research and articles. In this sense, understanding each case examined provides invaluable insights and explanations for understanding the topic of the object of study, and allows proposing strategies to improve the problem, which helps to put the topic in its respective context. The bibliography has been selected both for its usefulness in the present field of study and for its topicality, seeking to review the most important and current bibliographic material as possible.

Key words: Knowledge age, data protection, proactive responsibility, data protection officer, binding corporate standards, impact assessment

CONTENIDO: I. CONTEXTO GLOBAL.- II. EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA.- III. ALGUNOS EJEMPLOS DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA EN EL ÁMBITO DE LA UNIÓN EUROPEA.- III.1. DELEGADO DE PROTECCIÓN DE DATOS.- III.2. NORMAS CORPORATIVAS VINCULANTES.- III.3. EVALUACIÓN DE IMPACTO.- III.4 PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO.- IV. CONCLUSIONES.

I. CONTEXTO GLOBAL

La sociedad actual se conoce o denomina como «sociedad de la información». La información puede definirse como una serie de datos que, una vez procesados y organizados, dan lugar a un utensilio que proporciona la capacidad de modificar su estado de conocimiento a un sujeto o a un sistema. Por tanto, la sociedad de la información supone una transformación del propio término «información». Debe tenerse en cuenta que hoy en día, cuando hablamos de información, se trata de un concepto que el ser humano ha sido capaz de transformar a bits, a dígitos. Dicha transformación ha sido el artífice de un cambio sociológico y comunicativo sin precedentes: hablamos de la digitalización de la información.

Precisamente, esa capacidad de preparar la información en diversas formas (sonido, texto, imagen, etc.) y en un formato electrónico es el causante de que nuestra sociedad tenga a su disponibilidad un artefacto (el ordenador y su capacidad de interconexión) que configura y modifica la conceptualización que el ser humano tenía tanto del tratamiento como del acceso a la información. Esto ha generado, sin duda alguna, un cambio trascendente en nuestro entorno económico y social a nivel nacional e internacional.

Es importante que conste, además, que el término o idea de la «sociedad de la información» no es novedoso. Yoneji Masuda (1980), sociólogo y profesor japonés, ya lo venía utilizando desde los años ochenta del siglo pasado. Y lo hacía, precisamente, para hablar del nacimiento de

una época de la información basada en el uso de los ordenadores en conjunción con la tecnología de las comunicaciones (p. 197).

Sin profundizar en el ámbito sociológico, ya que excedería el objetivo del presente artículo, podemos señalar que «la Sociedad de la Información no se encuentra limitada únicamente a Internet, pero sí podemos decir, sin miedo a equivocarnos, que Internet es su máximo exponente» (Santamaría Ramos, 2011, p. 311). A la fecha, la sociedad actual ha incorporado a pasos agigantados una serie de tecnologías enfocadas en la comunicación interpersonal. Dicha situación, como no podría ser de otra forma, ha tenido claras repercusiones:

> El carácter físico de la economía se reduce. Si la era industrial se caracterizaba por la acumulación de capital, transformación de recursos en productos y en la propiedad física, en la nueva era lo estimable son las formas intangibles de poder que se presentan en paquetes de información y en activos intelectuales. El hecho es que se avanza en la desmaterialización de los productos físicos que durante largo tiempo fueron la medida de la riqueza en el mundo industrial (Terceiro & Matías, 2001, p. 260).

No puede quedar más claro que la economía se está transformando y que aparece un nuevo modelo económico, basado en el cambio de lo material a lo digital. Hoy en día, el mayor activo económico es aquel basado en la digitalización. Es más, tal cariz e importancia tiene este nuevo mundo digital en nuestra sociedad que las personas nos comenzamos a enfrentar al término «hiperconectividad», presentado por vez primera por los científicos canadienses Anabel Quan-Haase y Barry Wellman (2005, 2006) a raíz de sus estudios de comunicación de las organizaciones y sociedades en red.

La manifestación negativa de la hiperconectividad es la propia imposibilidad de desconectarse del uso de las herramientas tecnológicas. Dicha imposibilidad trunca por completo las rutinas y el día a día de las personas, a la par que provoca una conexión constante a internet que, a la postre, puede generar otros problemas derivados. No obstante, y a pesar de ciertas manifestaciones perniciosas, no podemos pasar por alto los múltiples beneficios que las tecnologías de la información y de las comunicaciones (TIC), así como la propia sociedad de la información, han traído a nuestra sociedad. El mayor de estos beneficios es el conocimiento, y es precisamente este concepto el que nos permite hablar de otro término de vital importancia para entender la sociedad actual: el de «sociedad del conocimiento». Hemos de entender que, hoy por hoy, la información y su aplicación se ven alterados para generar conocimiento. Las personas del siglo XXI ya no son receptoras de información de forma exclusiva, también son generadores de información.

La sociedad del conocimiento es la sucesora de la sociedad de la información. Esta aflora con el nuevo siglo y define una situación tecnológica, económica y social basada en la utilización y el uso del conocimiento. Además, se encuentra cimentada sobre cuatro factores: las tecnologías de la información y de las comunicaciones, la globalización, el uso del conocimiento para generar productos y servicios, y el aprendizaje de las entidades que han logrado mejorar su forma de organización.

El presente escenario es muy claro: el conocimiento es el motor, la energía de este sistema social, tanto desde el punto de vista económico como político. Se trata de un motor de cambio al que nadie puede permanecer ajeno, pues todos debemos adaptarnos a esta nueva sociedad del conocimiento. Dicho esto, debemos convenir en la necesidad de generar un espacio común que permita un progreso social y económico que produzca bienestar en las personas físicas.

Es en este contexto donde la información cobra un componente económico importante y toma especial relevancia la protección de datos de carácter personal. Actualmente, tenemos una normativa que sigue siendo —muy a nuestro pesar— de carácter local y que debiera ser de carácter global. En todo caso, esta debe tratar de equilibrar no solo el derecho de las personas a la protección de sus datos personales, sino también un adecuado progreso económico y social de carácter global.

Y hablamos de globalidad, algo que se trató de lograr en 1981 de lograr con el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que a través de su reciente modificación trata de buscar un escenario jurídicamente vinculante desde el punto de vista internacional. Su importancia ha sido tal que, a pesar de ser un convenio emanado del Consejo de Europa, ha sido firmado por Estados no miembros de dicho Consejo. Especial mención, en este sentido, merecen dos países latinoamericanos: Uruguay y Argentina, que firmaron el presente Convenio en los años 2018 y 2019, respectivamente. Este punto es de particular interés puesto que muestra claramente la voluntad de dichos países para ponerse a la vanguardia en la defensa de los derechos y las libertades inherentes a la protección de datos de carácter personal.

En este sentido, la Unión Europea ha decidido dar un paso adelante con su Reglamento relativo a la protección de datos, en el que puede observarse que estos criterios ya están incorporados a su ADN. Véase, por ejemplo, su considerando 6:

> La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen

> datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social […] (Parlamento y Consejo Europeo, 2016, p. 2).

O su considerando 7:

> un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades (Parlamento y Consejo Europeo, 2016, p. 2).

Téngase en cuenta que, en la Unión Europea, la protección de las personas físicas en relación con el tratamiento de sus datos de carácter personal se ha convertido en un derecho fundamental reconocido por la Carta de los Derechos Fundamentales de la Unión Europea en su artículo 8[1] (Parlamento y Consejo Europeo, 2000, p. 10).

Y no puede ser de otra forma, en el escenario global del siglo XXI esta protección es vital en el ámbito de las personas físicas, en tanto todas las organizaciones, ya sean públicas o privadas, tratan sin excepción datos de carácter personal durante el desarrollo de sus funciones y la consecución de sus objetivos. Pensemos que ninguna entidad hoy en día es capaz de desarrollar sus funciones y lograr sus objetivos sin el uso de la informática y de las telecomunicaciones.

Téngase en cuenta que el uso de las nuevas tecnologías ha añadido una dosis importante de comodidad y celeridad tanto en el procesamiento de los datos como en su intercambio, lo cual genera un importante trasiego de información a nivel mundial. Y es justo ese contexto el que genera una indefensión de las personas en relación a la protección de sus datos personales en todas las partes del mundo, ya sea que se disponga de legislación local en materia de protección de datos o no.

Afortunadamente para los europeos, se dispone en su ámbito local de una normativa fuerte, adaptada a los nuevos tiempos, pero a la que aún le queda mucho camino por recorrer. Cuestión distinta encontramos en el ámbito latinoamericano, donde la casuística es variada y se aprecian

1 Se reproduce el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea para mayor comodidad del lector: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

diferencias dispares. Así, tenemos países que disponen de normativa general de protección de datos como Argentina, Brasil, Chile, Colombia, Costa Rica, República Dominicana, México, Nicaragua, Panamá, Paraguay, Perú y Uruguay; pero también encontramos países que no cuentan con una normativa general de protección de datos como Bolivia, Ecuador, El Salvador, Guatemala, Honduras y Venezuela.

¿Qué podemos hacer en un entorno legislativo tan fraccionado, pero donde el elemento económico es de carácter global? Es decir, las normas son locales, pero las entidades públicas y privadas operan en un contexto internacional donde lo habitual es la captación, el tratamiento y, en su caso, la comunicación de datos de carácter personal. ¿Cómo podemos proteger adecuadamente los derechos de las personas en este escenario tan complejo?

En este sentido, se deben destacar los esfuerzos continuados de la Red Iberoamericana de Protección de Datos (RIPD) por lograr que Latinoamérica se convierta en un escenario en el cual tanto los actores privados como los públicos puedan desarrollar iniciativas y proyectos comunes en Iberoamérica. A la fecha, su máximo exponente ha sido la aprobación, en Santiago de Chile (junio de 2017), de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Red Iberoamericana de Protección de Datos, 2017, p. 4).

Los objetivos marcados por los presentes estándares son:

- Lograr una serie de principios y derechos comunes en materia de protección de datos para los Estados iberoamericanos.
- Garantizar el establecimiento de reglas comunes que permitan un efectivo ejercicio y tutela del derecho a la protección de datos de carácter personal dentro de los Estados iberoamericanos.
- Facilitar el flujo de datos personales entre los Estados iberoamericanos.
- Favorecer la cooperación internacional entre las autoridades de control de los Estados iberoamericanos.

La Unión Europea tuvo una idea que quizá sea posible exportar al ámbito latinoamericano. Hablamos del principio de responsabilidad proactiva, porque la protección de datos de carácter personal no debe ser teórica, no debe quedarse en el papel, pues las normas ya han demostrado sus carencias a nivel legislativo. Las normas de protección de datos de carácter personal, una vez entran en vigor, empiezan a perder su vigencia en tanto la práctica social y empresarial va generando nuevos riesgos y amenazas, impensables en el momento de pasar nuestra teoría al papel.

La protección de datos de carácter personal debe ser práctica en todas las organizaciones, basada en el día a día, centrada en responder a los retos más actuales; y eso solo pasa si hay una correcta cultura de protección de datos personales en el seno de las entidades, tanto públicas como privadas.

En la actualidad, las normas —el papel— por sí solas no son suficientes y es necesario activar mecanismos complementarios. Cierto es que la normativa europea cuenta con una ventaja con relación a los estándares citados anteriormente. Hablamos de normas de carácter supranacional y, «por tanto, de un ordenamiento jurídico que está por encima de los ordenamientos jurídicos de los Estados y que, por lo tanto, legaliza las instituciones comunitarias en la aplicación del derecho comunitario» (Biacchi Gomes *et al.*, 2018, p. 102). Esta es una cuestión muy diferente a cómo debemos entender los presentes estándares del ámbito intergubernamental pues, tal y como considera Calduch Cervera (1991), «la mayoría de las organizaciones intergubernamentales carecen de normas jurídicas susceptibles de imponerse a los ordenamientos jurídicos nacionales y a los ciudadanos de un modo directo» (p. 174).

La cuestión del poder coercitivo de una norma siempre es materia de interés en cualquier discurso jurídico. No obstante, basta para el presente artículo precisar que los reglamentos europeos son de aplicación directa en cualquier Estado miembro de la Unión Europea; mientras que los estándares emanados de la Red Iberoamericana de Protección de Datos, si bien tienen un alto valor por tratar de aportar unión y coherencia dentro de los Estados iberoamericanos en relación a sus aparatos legislativos, no dejan de suponer unas meras buenas prácticas que quedan, en lo que se refiere a su cumplimiento, sujetas a la decisión de los Estados, los cuales pueden o no seguir dichos criterios. Sin embargo, y a pesar del interés que puede tener —desde el punto de vista del derecho internacional público— la diferenciación entre normas emanadas de organizaciones supranacionales e intergubernamentales, hemos de declinar de entrar en debates de este tipo pues se alejan del núcleo central de la presente investigación.

II. EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

Lo primero que debemos destacar en relación con el principio de responsabilidad proactiva es que no es un término «moderno». Tal y como establece el Grupo de Trabajo del Artículo 29 (2010):

> Su reconocimiento expreso figura en las directrices sobre privacidad adoptadas en 1980 por la Organización de Cooperación y Desarrollo Económicos (OCDE). El principio de responsabilidad de estas reza así: "Todo responsable de datos debería ser responsable de cumplir con las

> medidas que hagan efectivos los principios [materiales] expuestos" […] (p. 7).

E incluso continúa, matizando que:

> Recientemente el principio quedó incluido en las Normas Internacionales de Madrid, desarrolladas por la Conferencia Internacional de Comisarios de Protección de Datos y Privacidad. Ha quedado también incorporado a la propuesta de norma más reciente de ISO 29100 […] (Grupo de Trabajo del Artículo 29, 2010, p. 7).

No obstante, el presente principio, a pesar de no ser novedoso, sino todo lo contrario, no ha sido aplicado por los responsables del tratamiento con toda la asiduidad que debieran. ¿Por qué? Pues porque los responsables del tratamiento únicamente se conforman con cumplir con las legislaciones locales establecidas en el país donde desarrollan su actividad.

Ahora bien, dicho esto, toca realizar la siguiente pregunta: ¿por qué las normas en materia de protección de datos no son eficientes? Simple y llanamente porque las entidades no aportan una auténtica protección de datos de carácter personal en el seno de sus instituciones. Y no es una cuestión personal o un juicio de valor, es lo que dice el Grupo de Trabajo del Artículo 29 (2010, p. 5), el mismo que, cuando habla de la responsabilidad como vector de una aplicación eficaz de los principios en materia de protección de datos de carácter personal, establece varias cuestiones de interés para comprender la presente cuestión, a saber:

- Las tecnologías de la información y de las comunicaciones han supuesto un escenario que el Grupo de Trabajo considera como «diluvio de datos». Los datos personales viajan a lo largo y ancho de nuestro planeta, por lo que cualquier responsable de su tratamiento necesita disponer de mecanismos eficaces que garanticen la protección de los datos personales.
- Estos datos de carácter personal se han visto revalorizados desde el punto de vista social, político y económico; es más, el Grupo de Trabajo resalta que hoy en día son incluso moneda de cambio, al punto de que las personas cambian sus datos personales por acceso a contenido. Por tanto, los datos son un producto de valor y eso hace necesario establecer medidas que salvaguarden la protección de datos de carácter personal.
- El presente escenario, tanto en el ámbito público como en el privado, puede generar filtraciones informativas con amplios efectos negativos. Es imprescindible para los responsables del tratamiento de datos disponer de una buena reputación y también de la confianza de las personas.

¿Por qué el principio de responsabilidad proactiva puede ser eficaz para cualquier tipo de institución? Porque el cumplimiento normativo de protección de datos no solo comporta el beneficio de evitar las posibles sanciones por su incumplimiento, sino que implica además beneficios importantes para la imagen y la reputación corporativa, genera una mayor confianza en los usuarios o clientes, y puede ayudar a minimizar riesgos y, con ello, optimizar nuestros recursos de carácter económico. Además, si esto es entendido por las instituciones públicas y privadas de todo el mundo, redundaría en una mejor protección de los datos personales de las personas físicas y lo haría con independencia del ámbito legislativo que tuviese que cumplir la entidad pública o privada en cuestión.

Por otro lado, es importante precisar que el principio de responsabilidad proactiva no supone hablar del principio de responsabilidad en general. En este sentido, es cierto que «el principio de responsabilidad implica, entonces, la asunción por parte del "responsable" y, en su caso, del encargado del tratamiento, de la normativa aplicable respecto a una serie de conductas que en ellos recaen como sujetos pasivos» (Rotondo Tornaría, 2019, p. 139). No obstante, esta responsabilidad es parte del principio de responsabilidad en general y nada tiene que ver con el principio de responsabilidad proactiva, que es algo totalmente diferente.

Como reseña claramente el Grupo de Trabajo del Artículo 29 (2010, p. 13) en el citado documento, el principio de responsabilidad proactiva supone hablar de un enfoque complementario al del principio general de responsabilidad, que incluiría una lista ilustrativa de medidas que se podrían fomentar a nivel nacional. De hecho, el propio Grupo de Trabajo del Artículo 29 hace mención expresa a las Normas Técnicas Internacionales adoptadas en Madrid[2] por las autoridades de protección de datos, que incluyeron en su artículo 22 una disposición sobre medidas de carácter proactivo que motivaron, siete años después, que el Reglamento General de Protección de Datos hable específicamente del principio de responsabilidad proactiva, el cual —insistimos— es un principio totalmente diferenciado del principio de responsabilidad general.

Es cuestión relevante significar y dejar claro que, obviamente, el principio de responsabilidad proactiva no supone acabar ni con las normativas de protección de datos ni, por supuesto, con sus principios más esenciales; únicamente supone aplicar un principio garantista a mayores, es decir,

2 Nos referimos a una Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, acogida favorablemente por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid. Esta se encuentra disponible para consulta a través del siguiente enlace: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

en beneficio de esa protección de las personas físicas en lo que respecta a sus datos de carácter personal. También creo relevante reseñar que el principio de responsabilidad proactiva puede completarse con otros mecanismos, también citados en el propio Reglamento General de Protección de Datos, como pueden ser las evaluaciones de impacto, el nombramiento de un directivo con responsabilidad en materia de protección de datos —denominado por el Reglamento como «Delegado de Protección de Datos»— o las normas corporativas vinculantes, mecanismos que pasaremos a mencionar y detallar más adelante.

Ciertamente, las Normas Técnicas Internacionales adoptadas en Madrid aportan una lista bastante detallada de medidas que podría ayudar a desarrollar el principio de responsabilidad proactiva (Autoridades de Protección de Datos y Privacidad, 2020), en concreto:

- Procedimientos de gobernanza o gestión de la seguridad de la información.
- Nombramiento de «funcionarios» de protección de datos.
- Programas de formación, educación y sensibilización para los miembros de la organización.
- Realización de auditorías transparentes.
- Adaptación de los sistemas de información del responsable del tratamiento a la legislación en materia de privacidad.
- Realización de evaluaciones de impacto.
- Adopción de códigos de prácticas.
- Aplicación de planes de respuesta que establezcan directrices de actuación ante una posible vulneración de la normativa de protección de datos de carácter personal.

Como podemos observar, el Reglamento General de Protección de Datos se ha nutrido de muchas cuestiones ya reflejadas en el presente documento, como los «funcionarios» de protección de datos —a los que posteriormente se ha denominado delegados de protección de datos—, las evaluaciones de impacto o los códigos de buenas prácticas; y también, cómo no, se han incluido nuevas cuestiones, como la protección de datos desde el diseño y por defecto.

En cualquier caso, se trata de que el responsable del tratamiento actúe en dos capas. Una primera capa, que podemos denominar «de mínimos», en la que el responsable del tratamiento centra sus esfuerzos en cumplir con la normativa en materia de protección de datos de carácter personal que le es de aplicación; y una segunda capa, que podemos denominar «de máximos», en donde el responsable del

tratamiento se torna en una figura proactiva que implementa, en el seno de su organización, una serie de sistemas facultativos de responsabilidad que proporcionan garantías más estrictas que las impuestas por la legislación.

Es cierto que cualquier individuo, sobre todo si suele ocupar la figura de responsable del tratamiento, puede tender a pensar que la responsabilidad proactiva es un principio que supone más costos que beneficios; y también que el responsable del tratamiento solo está obligado a cumplir con lo que le marca la legislación y, ciertamente, no tiene la obligación de ir más allá. En ese sentido, algo de razón tiene, pero solamente algo, porque ese tipo de pensamiento es no solo sesgado, sino también —permítaseme la expresión— «arcaico» en una época conocida como la era del conocimiento.

Pero lo cierto es que el principio de responsabilidad proactiva ha tenido que ser introducido en el ordenamiento jurídico para no dejar en manos del responsable del tratamiento un comportamiento o deber que, si bien debiera ser lo razonable desde el punto de vista ético, no resulta así para los responsables del tratamiento, cuya máxima es ceñirse a la legislación y, por tanto, al aparato coercitivo de la norma y no a la ética. De hecho, la Superintendencia de Industria y Comercio en Colombia ha realizado una interesante guía, titulada *Guía para la Implementación del Principio de Responsabilidad Demostrada*[3], que en esencia es una forma diferente para denominar al principio de responsabilidad proactiva establecido por el Reglamento General de Protección de Datos.

Precisamente, debemos de pensar en el porqué de las normas de protección de datos. Su finalidad es muy clara, como claro es el derecho coercitivo. Hay determinadas cuestiones que no se deben dejar en manos de la ética o de la buena fe, sino en manos del poder coercitivo del ordenamiento jurídico.

Vivimos es un entorno global. Hoy en día, los responsables del tratamiento no solo intentan cumplir con sus finalidades y objetivos en un área local (nacional), sino que tienden a hacerlo en un ámbito global (internacional); y eso es algo que conocen perfectamente sus clientes y usuarios. Los clientes y usuarios saben que las empresas que les prestan bienes o servicios ya no son entidades de carácter nacional, sino que con frecuencia son de carácter internacional. A ese factor se le añade el que las personas cada vez estemos más y mejor informadas, y que por tanto le demos valor a otras cuestiones. Ya no solo nos interesa un buen producto o servicio, sino también un buen servicio de posventa. Y, por supuesto, nos importa conocer y saber cómo, por qué y para qué se usan

3 Es posible localizar la citada guía en internet a través del siguiente enlace: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

nuestros datos de carácter personal; y, con más motivo, si esos datos van a ser utilizados por una compañía cuya razón social está radicada en un país que no es el del cliente o usuario.

Bien, a esa percepción que puede tener una persona hemos de añadir que el principio de responsabilidad proactiva no implica una mayor carga para el responsable del tratamiento. En esencia, este supone seguir cumpliendo con la normativa en materia de protección de datos de carácter personal, pero de una forma diferente y, si se quiere, con una mayor implicación del responsable del tratamiento, que no solo cumple sino que, además, instaura una cultura de protección de datos de carácter personal en el seno de su organización. Esto, a la larga, solo redunda en beneficio del responsable del tratamiento. Si en el seno de una organización existe una buena y correcta cultura en materia de protección de datos de carácter personal, los posibles incumplimientos tenderán a verse reducidos en dicha organización a mediano y largo plazo. Y esto se da precisamente porque todas las partes implicadas son conscientes de la importancia de la materia y darán la «voz de alarma» cuando consideren que ciertas acciones realizadas con los datos personales pueden estar vulnerando la normativa y los protocolos internos de actuación de la organización.

Además, aplicar el principio de responsabilidad proactiva en el seno de una organización también implica desarrollar una serie de elementos y herramientas que van a permitir a la entidad verificar y mejorar la calidad, así como la eficiencia y la efectividad de muchos de sus procesos, además de los relativos al tratamiento de los datos de carácter personal.

En consecuencia, un correcto diseño e implementación del principio de responsabilidad proactiva en el seno de una organización no debe ser visto por los responsables del tratamiento como una carga que no aporta beneficio alguno; al contrario, debe asumirse como un mecanismo que aporta evidencias claras y convincentes a la opinión pública de que dicha entidad desarrolla políticas en materia de protección de datos, las mismas que añaden un plus de garantía adicional en tanto van más allá de lo exigido por la normativa. Y eso, en un mundo globalizado donde los tratamientos son internacionales, pero la legislación es exclusivamente nacional, es valorado por las personas de una forma muy positiva.

Es cierto que debería existir una normativa internacional en materia de protección de datos dada esa internacionalización de los tratamientos, pero dicha normativa internacional que demandamos es hoy por hoy una utopía. Sin embargo, ante dicha utopía surge algo que no lo es, algo que es mucho más factible de implementar, y eso no es otra cosa que el principio de responsabilidad proactiva.

Un matiz importante por subrayar es el de la cuestión de las sanciones en materia de protección de datos. ¿Cumplir con el principio de responsabilidad proactiva implica quedar exento de sanciones en materia de protección de datos? Evidentemente, la respuesta es no. Que un responsable del tratamiento lleve a cabo una buena gobernanza en materia de protección de datos de carácter personal no significa que quede liberado por sus posibles incumplimientos en materia de protección de datos; otra cosa es que las autoridades de control no le impongan sanciones máximas o ejemplares por considerar que actúa de una forma más rigurosa y respetuosa de la normativa en sus tratamientos de datos de carácter personal.

Como ya comentamos anteriormente, el principio de responsabilidad proactiva, al menos en el ámbito europeo, no está dentro del campo de la ética sino dentro del campo del derecho.

III. ALGUNOS EJEMPLOS DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA EN EL ÁMBITO DE LA UNIÓN EUROPEA

En el presente acápite vamos a centrarnos en algunos ejemplos de cómo un responsable del tratamiento puede aplicar el principio de responsabilidad proactiva.

III.1. Delegado de protección de datos

En Europa, los artículos 37 a 39 del Reglamento General de Protección de Datos regulan lo que en castellano ha venido a traducirse como delegado de protección de datos, figura cuyo nombre tiene una mejor significación en el idioma de Shakespeare (*Data Protection Officer*) y que supone una expresión del principio de responsabilidad proactiva del cual venimos hablando.

Al igual que en el caso del principio de responsabilidad proactividad, no podemos olvidar que la presente figura no es nueva. Ya se encontraba regulada en la Directiva 95/46/CE y fueron no pocos Estados miembros de la Unión Europea los que decidieron transponerla a su derecho interno.

La Directiva 95/46/CE, en su texto en inglés, denominaba al actual delegado de protección de datos como *Data Protection Official*[4]. Este título hace referencia a aquella persona que se encuentra en posesión de una función o mandato —como parte de una organización o Gobierno—, y participa en el ejercicio de la autoridad cumpliendo el rol de lo que se suele denominar «directivo» en el ámbito de las organizaciones privadas; mientras que, en el de las organizaciones públicas, cumple el papel de

4 En castellano, el término *official* tiene una clara vocación de «persona al mando», con auténtica potestad de decisión.

aquellos individuos con potestades directivas y de organización de corte fundamentalmente político en tanto sus cargos son de confianza y, por tanto, han sido elegidos por quienes ostentan el poder político. En suma, hablamos de una figura que, en esencia, corresponde a una persona que ocupa un cargo directivo y a la que se le encomienda la tarea de vigilar el cumplimiento de la legislación en materia de protección de datos en una determinada organización, pública o privada, que con motivo de sus actividades trata datos personales.

En este sentido, el legislador europeo ha establecido un sistema dual en el que el delegado puede tener un carácter interno y, por lo tanto, sometido a una relación de carácter laboral con el responsable del tratamiento; o bien ser de carácter externo y, por lo mismo, estar sujeto a una relación estrictamente mercantil.

Una de las cuestiones reflejadas por el Reglamento General de Protección de Datos tiene que ver con que el delegado de protección de datos pueda ejercer sus funciones con plenas garantías y, para ello, se hace imprescindible que sea independiente; es decir, que mantenga una postura imparcial y objetiva, siguiendo los criterios básicos de un auditor.

Para ello, vamos a apoyarnos en el ejemplo de los auditores de cuentas. Bajo esta lógica:

> Los auditores de cuentas deberán ser y parecer independientes, en el ejercicio de su función, de las empresas o entidades auditadas, debiendo abstenerse de actuar cuando su objetividad en relación con la verificación de los documentos contables correspondientes pudiera verse comprometida (Lara Bueno, 2008, p. 36).

Si procedemos a traducir el presente principio al lenguaje de la protección de datos de carácter personal, podemos decir que el delegado de protección de datos

> deberá ser y parecer independiente, en el ejercicio de sus competencias, de las empresas o entidades en las que realice sus funciones, debiendo abstenerse de actuar cuando su objetividad *en relación a la protección de los datos de carácter personal* pudiera verse comprometida (Santamaría Ramos, 2011, p. 381)[5].

Esto quiere decir que la persona que ostente el cargo deberá desarrollar su trabajo de forma autónoma, sin encontrarse sujeto a coacciones de ningún tipo, actuando libremente y ejerciendo sus funciones —saber y entender— en virtud de su experiencia, de manera que pueda desarrollarlas de forma objetiva y con plenas garantías. Además, durante el ejercicio de sus funciones tendrá el derecho y la obligación de exponer sus

5 Énfasis añadido.

criterios y realizar las recomendaciones que considere oportunas, no viéndose obligado a adoptar decisiones o procedimientos con los que no se encuentre de acuerdo o que pudiesen causar algún perjuicio[6] a la entidad en la que desarrolla sus funciones.

Como podemos observar, la independencia se configura, por tanto, como un principio fundamental para la figura del delegado de protección de datos, así como para el principio de responsabilidad proactiva.

Es cierto que el Reglamento General de Protección de Datos no menciona de forma expresa el principio de independencia del delegado de protección de datos, aunque hemos de decir en su favor que sí lo refiere de manera indirecta cuando su artículo 38.3 establece que «el responsable y el encargado del tratamiento garantizarán que el Delegado de Protección de Datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones» (Parlamento y Consejo Europeo, 2016, p. 56).

Asimismo, una de las mayores carencias que se observa en toda la regulación de la labor del delegado de protección de datos, y de manera particular en el artículo relativo a su designación, es que no se establece una limitación de la duración del mandato o la asunción de funciones del delegado en cuestión. Parece ilógico que si el principio de independencia está presente en esta figura, no se encuentre previsto que la misma debe ser matizada y definida temporalmente durante un periodo que le permita ejercer sus funciones con total imparcialidad e independencia.

En este sentido, lo más conveniente es que el mandato dure menos de cuatro o cinco años, de forma que se proteja a esta figura de presiones que puedan menoscabar la teórica neutralidad de sus funciones (Magide Herrero, 2000, p. 95), independientemente de que sea un delegado de carácter interno o un delegado de carácter externo. Téngase en cuenta que un periodo de tiempo inferior podría entenderse como un lapso insuficiente para garantizar la objetividad del puesto, mientras que uno mayor podría generar una pérdida de imparcialidad de la persona física que ostenta el cargo.

Es necesario tener en cuenta que el delegado de protección de datos adquiere un rol de especial importancia, especialmente porque sobre ella recae la gran responsabilidad de configurar un sistema organizativo que permita al responsable del tratamiento ejercer su actividad, respetando la legislación en materia de protección de datos de carácter personal. Por esta razón, deberá ser una persona con altos conocimientos técnicos

6 Entendiendo por perjuicio cualquier acción u omisión que pueda provocar que el responsable del tratamiento incurra en una infracción en materia de protección de datos de carácter personal, conforme a la legislación vigente.

y una experiencia profesional contrastada en el ámbito del derecho y las nuevas tecnologías.

La Decisión de la Comisión del 3 de junio de 2008 aporta, en su artículo 3.4, una descripción básica de la presente figura:

> deberá tener sólidos conocimientos de los servicios y estructura de la Comisión y de sus normas y procedimientos administrativos. Tendrá que conocer bien los sistemas, principios y metodologías de la protección de datos y la información. Deberá demostrar que tiene sentido común y es capaz de mantener una postura imparcial y objetiva conforme al Estatuto de los funcionarios (Comisión de las Comunidades Europeas, 2008, p. 8).

Cierto que la figura establecida por la mencionada Decisión no se refiere, en concreto, a la nueva figura del delegado de protección de datos establecida por el Reglamento General de Protección de Datos, pero no es menos cierto que lo dicho en el citado artículo para un responsable de protección de datos es perfectamente aplicable al delegado de protección de datos.

Aunque el artículo 37 del Reglamento General de Protección de Datos no lo diga expresamente, la persona que ejerza el cargo de delegado debe encontrarse formada en una gran variedad de conocimientos que aborden los tres ámbitos que la normativa en materia de protección de datos de carácter personal abarca: jurídico, técnico y organizativo. A su vez, como características intrínsecas a la personalidad de este individuo, deberá demostrar capacidad de juicio imparcial y objetiva.

Desde el punto de vista «jurídico», es necesario que la persona disponga de un amplio conocimiento de la normativa en materia de protección de datos de carácter personal y de su aplicación al caso concreto. Además, el delegado de protección de datos debe disponer de una alta capacidad para la redacción jurídica, siendo necesaria una redacción clara y concreta que exprese con concisión las ideas y puntos clave, así como la aptitud para crear con fluidez sus propios textos jurídicos puesto que, en una materia como la que nos ocupa, los modelos o formularios jurídicos no podrán ser aplicados al caso concreto en la mayoría de las ocasiones.

Desde el punto de vista «técnico», es imprescindible que la persona que ocupe el cargo se encuentre formada en tecnologías de la información y la comunicación. En concreto, deberá encontrarse en posesión de los conocimientos básicos para seleccionar las herramientas TIC más apropiadas para ser vinculadas a los procesos de trabajo llevados a cabo por la organización. En este contexto, no será imprescindible que la persona que desarrolla las tareas del delegado tenga la categoría de ingeniero o experto en informática, pero sí será conveniente que disponga de conocimientos suficientes que le permitan tomar las decisiones correctas

o más acertadas en lo relativo al uso de la tecnología en la organización. En particular, sus conocimientos deberán encontrarse dirigidos a:

- La aplicación de las tecnologías de la información y la comunicación en las organizaciones de cara a relacionarlas con la actividad, las estrategias, y los procesos organizativos y de trabajo en la organización.
- El manejo de las aplicaciones informáticas básicas o usuales en cualquier entorno organizacional.
- El conocimiento de los sistemas de información y las redes en todos los temas referidos a su integración y funcionamiento.
- La utilidad, el funcionamiento y la integración de los sistemas de comunicación electrónicos: correo electrónico, telefonía IP, sistemas de videoconferencia, etcétera.
- La seguridad de los sistemas y la protección de la información, y en especial del conocimiento, frente a los riesgos más comunes, así como de los conocimientos básicos para su prevención.

En general, se valorará que la persona en el cargo disponga de los conocimientos técnicos necesarios para establecer políticas, procedimientos y prácticas que, desde un punto de vista organizativo o directivo, prevengan, detecten y, en última instancia, sean capaces de corregir los sucesos perjudiciales producidos en entornos tecnológicos en materia de protección de datos de carácter personal.

Desde el punto de vista «organizativo», se hace necesario considerar que la persona que ejerce el cargo de delegado de protección de datos deberá disponer de habilidades en lo relativo a la gestión y dirección de proyectos y recursos humanos, así como conocimientos relacionados a la organización y gestión de las tecnologías de la información; es decir, saberes dirigidos a la gestión íntegra y global (Pereña Brand, 1996, p. 60). En esencia, el perfil organizativo de esta figura jurídica se centra en generar una actitud dinámica, cuya finalidad última sería la mejora de los procesos de interacción organizativos orientados a la consecución de la mayor efectividad posible. Por lo tanto, la persona que ejerza las funciones propias de este puesto deberá encontrarse familiarizada con las habilidades y herramientas relativas a la gestión directiva, en concreto:

- Organización y buenas prácticas en la gestión y seguridad de las tecnologías de la información.
- Definición de políticas, controles y procedimientos tanto en entornos tecnológicos como de gestión de los recursos humanos.
- Conocimientos básicos de organización empresarial.

- Planificación estratégica, entendida como el proceso directivo tendente a lograr un equilibrio entre los objetivos de la organización, los recursos y las oportunidades cambiantes del mercado que, en el ámbito que nos ocupa, deben ser a su vez entendidas como las múltiples variables (tecnológicas, sociales, legales…) que pueden afectar la protección de datos de carácter personal.
- Organización y gestión de equipos y tareas.
- Liderazgo y dirección de personas.
- Negociación y comunicación.
- Gestión del cambio o, lo que es lo mismo, aplicación de determinados métodos en una organización para adaptarla a los nuevos retos que plantea la sociedad de la información.

Sin duda alguna, la formación en los tres aspectos marcados por la legislación en materia de protección de datos de carácter personal: jurídico, técnico y organizativo, es indispensable para cualquier persona que quiera ejercer las funciones propias de un delegado de protección de datos. No obstante, existen dos puntos fundamentales que van más allá de la formación y que es necesario considerar a la hora de seleccionar a la persona idónea para ocupar el cargo: las habilidades personales y la experiencia profesional.

En relación con el primer elemento, se hace preciso tener en cuenta que el ser humano, a medida que se desarrolla como persona y dependiendo del contexto, adquiere una serie de habilidades para enfrentar y superar los retos personales y profesionales; es lo que conocemos como habilidades personales. En esta línea, sería deseable que la persona designada para desarrollar las tareas y funciones de un delegado de protección de datos contase con las siguientes habilidades:

- Habilidad para documentar y evidenciar las tareas y procesos llevados a cabo. Esto implica no solo un alto grado de concentración, sino que además requiere que la persona sea altamente ordenada y meticulosa.
- Habilidades comunicativas y argumentativas.
- Carácter mediador o la competencia para resolver conflictos, dado que en una materia tan compleja como la protección de datos de carácter personal es frecuente que aparezcan posturas encontradas. Corresponderá al delegado de protección de datos resolver dicho conflicto, procurando la satisfacción de ambas partes; es decir, intentando «manejar el ambiente tenso y emocionalmente cargado, típico de la mayor parte de las confrontaciones interpersonales» (Whetten & Cameron, 2005, p. 347).

En relación con el segundo elemento, es conveniente que la persona seleccionada para el puesto hubiese desempeñado con anterioridad:

- Funciones en áreas o departamentos relativos a las tecnologías de la información y las comunicaciones.
- La dirección de proyectos, lo que supone haber desarrollado funciones encaminadas a la ejecución de un proyecto en el tiempo establecido, dentro de los alcances delimitados y ajustándose al presupuesto y las especificaciones preestablecidas.
- Labores relacionadas con la implantación de procedimientos de control internos encaminados a la correcta utilización y destino de los recursos de la organización, sin que sea necesario que dicha experiencia profesional se haya dado en el campo de la implantación de procedimientos en ámbitos relativos a la protección de datos personales.
- La abogacía en materias referidas al ámbito del derecho informático o, si no es el caso, la participación como consultor o asesor en proyectos relativos a la protección de datos de carácter personal.

Como ya hemos comentado, la presente figura se encuentra establecida como una obligación legal dentro de la Unión Europea, tal y como establece el propio Reglamento General de Protección de Datos. En este mismo sentido, interesa matizar que, en el ámbito latinoamericano, la presente figura ha sido incluida dentro del ordenamiento jurídico de Uruguay, en concreto en el capítulo IV del decreto N° 64/2020 —que reglamenta la ley de protección de datos personales (Ley N° 18.331)—, aprobado en febrero de 2020. Esto supone un importante avance en el ámbito que nos ocupa pues, por vez primera, la presente figura se normativiza en el ámbito latinoamericano y dicha cuestión debe ponerse en valor. Incluso, la presente norma arroja algo de luz sobre un concepto realmente indeterminado y al que no se ha puesto coto en la Unión Europea: el concepto de «gran volumen» de datos personales, que la presente norma establece en datos de más de 35 000 personas. Si bien es posible aventurarse a criticar si esta definición es correcta o no, desde nuestro punto de vista es mucho mejor tratar de definir el concepto —a riesgo de equivocarse— que no definirlo, siendo esto último lo que sucede en la normativa europea. En todo caso, la presente figura ya se encuentra dentro del ordenamiento jurídico uruguayo y eso es, quizá, lo más importante: caminar hacia ordenamientos jurídicos homogéneos.

III.2. Normas corporativas vinculantes

Las *binding corporate rules*, o normas corporativas vinculantes, se establecen como la alternativa a las cláusulas contractuales tipo para

legitimar las transferencias internacionales de datos entre grupos de empresas multinacionales cuyas filiales se encuentren establecidas en países situados fuera del territorio de la Unión Europea o del Espacio Económico Europeo. No debemos olvidar en este punto que una empresa multinacional:

> Está compuesta por diversas sociedades que tienen diferenciada su personalidad jurídica, de modo que cada una tiene la suya, a pesar de que una sociedad mercantil esté participada por otra y, por tanto, cada sociedad mercantil es responsable de sus tratamientos de datos de carácter personal y debe aplicar la normativa de protección de datos con respecto de sus tratamientos (Santos García, 2005, p. 40).

Estas normas tienen su origen en la aprobación del documento de trabajo N° 74 (WP 74) por parte del Grupo de Trabajo del Artículo 29, que nace fruto de las constantes sugerencias que desde el sector empresarial, y fundamentalmente las organizaciones multinacionales, abogaban por considerar que la expresión «garantías adecuadas», propuesta en el artículo 26.2 de la Directiva 95/46/CE, «suponía dar cabida, no solo a las cláusulas contractuales tipo sino a una serie de códigos de conducta o de buenas prácticas, de carácter vinculante, que podrían ser suscritas entre las entidades comunitarias y sus filiales extracomunitarias» (Grupo de Trabajo del Artículo 29, 2003, p. 10).

Las compañías multinacionales tenían la convicción de que las medidas de carácter unilateral, al ser capaces de desplegar y garantizar una serie de efectos jurídicos en relación a la protección de los afectados o interesados en lo relativo a las transferencias internacionales de datos, podrían ser explotadas y tendrían plena cabida dentro del artículo 26.2, máxime cuando era factible articular además la intervención de las autoridades de control nacionales. De esta forma, si una organización multinacional se encontraba en disposición de demostrar su absoluto control sobre sus filiales al ser capaz de obligarlas a cumplir una serie de políticas de carácter interno —entre las que pueden encuadrarse aquellas destinadas a la protección de datos—, se podía recurrir a las normas corporativas vinculantes en sustitución de las cláusulas contractuales. Por ello, el Grupo de Trabajo del Artículo 29 utiliza el término «normas corporativas vinculantes» para «enfatizar el hecho de que estas reglas tienen realmente efectos legales» (Morgan & Boardman, 2008, p. 166).

Las sugerencias de las compañías multinacionales no fueron desatendidas por el Grupo de Trabajo del Artículo 29, que el 3 de junio de 2003 aprobó el citado documento de trabajo N° 74, en el que además el Grupo se decantó por considerar que la expresión «garantías adecuadas» del artículo 26.2 debía interpretarse como un concepto amplio que abarcaba no solo las soluciones contractuales (cláusulas tipo) y las normas corporativas vinculantes, sino que además se podía encuadrar

dentro del mismo cualquier otra solución que las autoridades de control puedan considerar convenientes para habilitar las transferencias internacionales de datos a países que no garanticen un adecuado nivel de protección.

Por cierto, no se debe caer en el error de considerar que las normas corporativas vinculantes vienen a sustituir o dejar sin vigencia las soluciones contractuales, sino que suponen una ampliación del abanico de posibilidades para realizar transferencias internacionales de datos, e incluso pueden combinarse entre sí para garantizar la eficacia jurídica.

Es cierto que las normas corporativas vinculantes guardan cierta similitud con los códigos de conducta; sin embargo, esto no significa que sean equivalentes. Los códigos de conducta son un conjunto de normas dirigidas a la aplicación práctica, en un sector profesional determinado, de la normativa nacional en materia de protección de datos de carácter personal. Su finalidad consiste en ofrecer un instrumento de autorregulación que permita establecer soluciones eficaces a los puntos conflictivos que presenta la aplicación de la normativa en determinados sectores profesionales.

Por el contrario, las normas corporativas vinculantes tienen una finalidad radicalmente opuesta a la de los códigos de conducta, partiendo de la base de que en ningún caso pueden sustituir a las obligaciones legales a las que se encuentran compelidas las organizaciones en virtud del derecho nacional y que deben ajustarse, en la medida de lo posible, a los principios que inspiran el Reglamento Europeo de Protección de Datos. Así, las normas corporativas vinculantes tienen su razón de ser en las transferencias internacionales de datos y su objetivo específico radica en flexibilizarlas y simplificarlas.

En segundo lugar, hemos de destacar su carácter global, lo que implica que su contenido debe ser aplicado por todo el conjunto de organizaciones del grupo, con independencia de su lugar de establecimiento, así como de la nacionalidad de los interesados o afectados cuyos datos están siendo tratados. Además, «no debemos olvidar su carácter vinculante, es decir, legalmente exigible en su conjunto» (Burnett, 2009, p. 163), tanto a nivel interno —de obligado cumplimiento para todo el personal del grupo empresarial— como a nivel externo —cualquier afectado o interesado puede exigir su efectivo cumplimiento—.

Parte de su esencia y, sin duda, de su eficacia reside en que las normas corporativas vinculantes se encuentren en posesión de las facultades que permitan resolver dos problemas fundamentales: de un lado, su cumplimiento a nivel interno y, de otro, su exigibilidad jurídica a nivel externo. A nivel interno, no cabe duda de que su carácter vinculante reside en que tanto los miembros del grupo empresarial —es decir, cada una de las empresas— como el personal adscrito a las mismas se

sientan compelidos a cumplirlas; por lo tanto, estas normas deberán contar con sanciones disciplinarias oportunas para los empleados y las organizaciones infractoras, así como con un programa eficaz de formación y concienciación para todos los elementos implicados, sean estos empleados, directivos, empresas prestadoras de servicios, etcétera.

Lo dicho anteriormente se convierte en un elemento vital para aquellas entidades filiales de la organización establecidas en países que no garantizan un nivel adecuado de protección o están fuera del ámbito de la Unión Europea o del Espacio Económico Europeo. En dicho caso, las diferencias legislativas y culturales se van a convertir en la principal barrera o escollo al cual se van a enfrentar las normas corporativas vinculantes, teniendo el grado de incumplimiento mayores probabilidades de asentarse si no se adoptan las medidas formativas, primero, y sancionadoras, en segundo lugar. La elaboración de la normativa interna debe responder a criterios prácticos y realistas, ya que debe encajar perfectamente con la filosofía y las actividades de las organizaciones de países que no cumplen con el adecuado nivel de protección; por lo mismo, deben ser lo suficientemente claras para que el personal las comprenda y puedan ser aplicadas eficazmente por todos aquellos trabajadores que durante el desarrollo de sus funciones traten datos de carácter personal. Corresponderá a la sede europea o, en su caso, a las organizaciones radicadas en la Unión Europea, redactar normas internas lo suficientemente claras y concisas, teniendo en cuenta que la finalidad principal es lograr un efectivo cumplimiento en el resto de entidades radicadas fuera de la Unión. De igual manera, se debe tener en cuenta que todo el peso y la responsabilidad de garantizar que cualquier entidad extracomunitaria ajuste sus tratamientos de datos personales a lo establecido en las normas corporativas vinculantes, asumiendo además su posición de garante del cumplimiento, recaerán sobre las entidades radicadas en la Unión Europea. De esa manera, en caso de incumplimiento, serán ellas mismas las que deberán responder sobre la exigibilidad jurídica en aquellos supuestos en los que los afectados o interesados consideren que sus derechos han sido vulnerados, o cuando las autoridades de control nacionales consideren que existen tratamientos que no se adecuan a los principios establecidos por el Reglamento General de Protección de Datos.

La solución reside, como ya hemos adelantado, en que una de las organizaciones localizadas en el territorio de la Unión, ya sea la casa matriz o una filial, asuma la responsabilidad de adoptar las medidas que estime oportunas para remediar las acciones de cualquier miembro del grupo empresarial radicado fuera de la Unión Europea y, de ser el caso, pagar la posible indemnización por los daños ocasionados con motivo de la infracción de las normas corporativas vinculantes. Por tanto, la organización europea debe ser consciente de la posibilidad de verse

sometida a un proceso sancionador con motivo de los tratamientos realizados por cualquiera de las compañías pertenecientes a su grupo empresarial radicadas fuera de la Unión, o bien a consecuencia de que un afectado o interesado considere que los procedimientos del grupo empresarial no han sido ejercidos con la correspondiente diligencia en aras de la preservación de sus derechos. La exigibilidad de las normas corporativas vinculantes parte de una premisa básica: «su transparencia, traducida en términos de lealtad y coherencia» (Nieto Tamargo & Iglesias González, 2000, p. 150).

Por otro lado, los afectados o interesados han de encontrarse totalmente informados de cuáles son las políticas del grupo empresarial en materia de protección de datos de carácter personal, en particular si es que sus datos van a ser comunicados a empresas del grupo establecidas en países situados fuera del ámbito de aplicación del derecho comunitario y, por lo mismo, fuera de su legislación nacional. Además, no debemos olvidar que la solución unilateral conformada por las normas corporativas vinculantes, unida a la necesaria cooperación entre el grupo empresarial y las autoridades de control nacionales, no elimina la posibilidad de que el interesado pueda recurrir a la jurisdicción ordinaria. Esto se puede dar fundamentalmente por dos razones: en primer lugar, porque ningún sistema puede garantizar con exactitud el cumplimiento efectivo de las normas y, por tanto, los afectados o interesados no tienen por qué estar necesariamente de acuerdo con la resolución tomada; y, en segundo lugar, porque las autoridades de control en ningún caso tienen la competencia para conceder una indemnización por los daños y perjuicios ocasionados, competencia que corresponde en exclusiva a los jueces y tribunales.

Sin embargo, tal y como considera el Grupo de Trabajo del Artículo 29, las normas corporativas vinculantes han de conceder una mayor importancia a la autorregulación del sistema. De esta forma, tiene que ser el grupo corporativo el que en la práctica asuma el cumplimiento efectivo de su normativa interna, si bien es necesario establecer la posibilidad de que el afectado o interesado pueda recurrir a la justicia ordinaria en algunas situaciones.

Asimismo, debemos tener en cuenta que las organizaciones multinacionales no son estáticas; al contrario, «están basadas en un sistema dinámico operacional» (Trigo Chacón, 2005, p. 32), lo que implica en algunas ocasiones la adquisición de nuevas compañías o la creación de filiales en diversas partes del globo como forma de ampliar sus oportunidades de negocio. Esto significa que la normativa interna debe ser proclive a tener en cuenta las particularidades culturales y también a la hora de abarcar procesos de sensibilización en materia de protección de datos. Cada entidad, e incluso cada país, tiene sus

particulares formas de actuar en este sentido. En esa línea, el Grupo de Trabajo del Artículo 29 considera que las modificaciones en las normas corporativas vinculantes son posibles siempre y cuando se cumplan las siguientes condiciones:

- No se realizará ninguna transferencia internacional de datos a nuevos miembros hasta que estos se sometan a las normas corporativas vinculantes, lo cual implica inexorablemente su aceptación y conformidad.
- Los nuevos miembros deberán nombrar a una persona o departamento específico, al cual competerá la tarea de confeccionar una lista actualizada de los miembros de la corporación, realizar un seguimiento y registro de todos los cambios generados en las políticas internas, y proporcionar información a los afectados o interesados; o, de ser el caso, a las autoridades de control nacionales cuando estas lo requieran.
- Informar a la autoridad de control competente, al menos con una periodicidad anual, de cualquier cambio en las normativas corporativas vinculantes o en la lista de miembros de la corporación multinacional. Esta data que deberá ir acompañada de un breve informe en el que se justifique la necesidad de la actualización.

Una vez analizadas las características básicas de las normas corporativas vinculantes, debemos pasar a analizar su contenido. Para garantizar los principios establecidos por el Reglamento General de Protección de Datos en relación al tratamiento de datos personales en organizaciones internacionales con sedes o compañías radicadas en países que no ofrecen una adecuada protección, las normas corporativas vinculantes deben contener:

- *Un sistema que garantice el conocimiento y la aplicación de las normas, tanto dentro como fuera de la Unión Europea*. Por tanto, cualquier corporación multinacional que incorpore dentro de sus políticas internas una norma relativa a la transferencia internacional de datos deberá conformar un conjunto de instrucciones precisas que asegure que estas son conocidas, entendidas y aplicadas de forma eficiente y eficaz en todas sus organizaciones y, consecuentemente, por todos sus empleados. Así, será necesario establecer procesos informativos y de formación oportunos para los empleados, además de crear un grupo especializado en materia de protección de datos de carácter personal que supervise y garantice la correcta aplicación de las políticas internas.
- *Establecimiento de un sistema de auditorías*. Nos referimos a un sistema de auditorías completo en el que se revisará —bien de

forma interna, bien de forma externa— el cumplimiento de las normas corporativas vinculantes a nivel jurídico, técnico y organizativo. La auditoría deberá concluir con la elaboración de un informe en el que se detallen los posibles incumplimientos en materia de protección de datos de carácter personal y sus medidas de corrección, así como las propuestas de mejora que el auditor considere necesarias. Dicho informe deberá ser entregado a la compañía radicada dentro de las fronteras de la Unión Europea, que deberá mantenerlo a disposición en caso sea requerido por la autoridad de control nacional competente. En este sentido, y de cara a garantizar la imparcialidad del informe de la auditoría, sería posible que las propias autoridades de control nacionales realizasen la inspección y elaboración del informe con consentimiento del grupo empresarial, sin que esto suponga necesariamente la imposición de sanciones como consecuencia de las infracciones detectadas. Es más, la elaboración de las auditorías por parte de las autoridades de control supondría la buena voluntad y transparencia, por parte de los grupos empresariales, de cumplir con los principios estipulados en materia de protección de los datos de carácter personal. La labor de las autoridades de control nacionales, por su parte, no sería detectar y sancionar los incumplimientos en la materia, sino detectar los incumplimientos y ayudar a los grupos empresariales a mejorar y corregir sus tratamientos, evitando las sanciones y cooperando estrechamente con estos para lograr normas corporativas vinculantes eficaces y respetuosas con los principios en materia de protección de datos.

- *Procedimiento de tramitación y resolución de las quejas planteadas por los afectados o interesados*. Este es un punto de especial relevancia en el que no solo será necesario detallar los pasos necesarios a seguir a nivel interno, sino que además exige contemplar mecanismos de resolución externos para aquellos casos en los que los afectados o interesados no estén de acuerdo con la solución estipulada por el grupo empresarial. En este contexto, sería interesante recurrir a las posibilidades que la institución del arbitraje ofrece, haciendo partícipes a las autoridades de control nacionales. Sería un «sistema arbitral que incluso puede realizarse on-line» (Gonzalo Quiroga, 2003, p. 48), en el que deja de tener sentido plantearse dónde tiene lugar el arbitraje, lo cual no deja de ser útil en un escenario como el aquí planteado.
- *Mecanismos de cooperación con las autoridades nacionales de control*. Las normas corporativas vinculantes deberán contener la obligación clara de cooperar con las autoridades de control nacionales o, si se prefiere, establecer una «sinergia entre la

acción pública y la acción privada» (Sainz Moreno, 2004, p. 112), de forma que todo el grupo empresarial, tanto a nivel global como individual, se comprometerá a seguir las instrucciones y consejos de la autoridad de control nacional competente en torno a aquellos temas relacionados con la interpretación y aplicación de las normas corporativas vinculantes establecidas por el grupo. Este mecanismo supondría una clara predisposición, tanto por parte del grupo empresarial como de sus elementos, de mantener unas políticas internas transparentes que velen por garantizar el tratamiento de los datos personales; y, al mismo tiempo, una predisposición de las autoridades de control a dejar en un segundo plano su competencia sancionadora para sustituirla por un marcado carácter dialogante y cooperativo que ayude al grupo empresarial a cumplir con la legislación vigente. La colaboración se traduce, en el caso de las autoridades de control, a elaborar recomendaciones dirigidas al grupo empresarial en su conjunto o a alguno de sus elementos, ya sea en respuesta a las preguntas realizadas por el grupo con motivo de una posible reclamación o denuncia de un afectado o interesado, o bien por iniciativa propia de la autoridad de control al detectar alguna situación que pudiese ver comprometidas las garantías de las normas corporativas vinculantes. Por cierto, que la potestad sancionadora de las autoridades de control quede en un segundo plano no significa que esta no deba ejercitarse. En aquellos casos en los que el grupo empresarial o alguno de sus elementos incurriese en una infracción grave o en una persistente negativa a cooperar, o incumpla las recomendaciones estipuladas por la autoridad de control, ello deberá suponer una sanción que, en función de la gravedad, conlleve incluso la pérdida de vigencia de las normas corporativas vinculantes y, por tanto, la imposibilidad de que el grupo empresarial pueda realizar transferencias internacionales de datos a países que no ofrezcan un adecuado nivel de protección. Cabe precisar que las normas corporativas vinculantes suponen una «posición de privilegio», fundada en la buena fe y la predisposición del grupo empresarial; por ello, si estas premisas se pierden, el grupo empresarial deberá volver a regirse por el Reglamento General de Protección de Datos en lo relativo a las transferencias internacionales. En todo caso, como no podría ser de otra manera, esta decisión deberá tener la forma de acto administrativo y, por tanto, dicha decisión podrá ser recurrida ante los juzgados y tribunales competentes.

- *Responsabilidad y sanciones*. Las normas corporativas vinculantes deberán establecer disposiciones relativas a la responsabilidad y competencia, de cara a facilitar a los afectados o interesados

el ejercicio práctico de las disposiciones establecidas por el Reglamento General de Protección de Datos. El elemento del grupo empresarial que resida dentro de la Unión Europea, que puede o no ser la empresa matriz, deberá aceptar la responsabilidad sobre todos los tratamientos efectuados por el grupo, así como obligarse a adoptar cuantas medidas se estimen necesarias para remediar los incumplimientos de cualquier otro miembro del conglomerado, en cuyo caso deberá pagar una indemnización o sanción por los daños resultantes de la violación de los principios establecidos por el Reglamento o con motivo de la reclamación de un afectado ante la autoridad nacional de control competente.

- *Transparencia*. Se deberán habilitar mecanismos que permitan a los afectados obtener la información relativa a la comunicación de sus datos personales a los demás elementos del grupo empresarial, entre los que se encuentran compañías ubicadas en países que no ofrecen un adecuado nivel de protección de estos datos. Esto se hará sobre la base del establecimiento de políticas internas (normas corporativas vinculantes) legalmente exigibles y que se encuentren autorizadas por la autoridad de control competente. De esta forma, se cumplirán las previsiones establecidas por el Reglamento General de Protección de Datos relativas al deber de información para con el afectado o interesado.

Sin duda alguna, las normas corporativas vinculantes suponen una fórmula idónea para flexibilizar y simplificar las transferencias internacionales de datos a escala mundial con base en un sistema autorregulador cimentado en su exigibilidad jurídica, tanto a nivel interno como externo, y en la capacidad de cooperación entre los grupos multinacionales y las autoridades de control nacionales.

Interesa matizar que las normas corporativas vinculantes están completamente diferenciadas de otra cuestión similar: la consideración de «país adecuado», y eso teniendo en cuenta que ambos mecanismos se consideran de garantías adecuadas a efectos de la realización de transferencias internacionales de datos. En este sentido, debe tenerse en cuenta que la decisión de considerar o no un país como adecuado emana, en el caso de la Unión Europea, de un estudio realizado por la Comisión Europea en cada caso. En otras palabras, dado que la potestad de declarar que un país no miembro de la UE garantiza un adecuado nivel de protección de los datos personales corresponde en exclusiva a la Comisión Europea, que es la encargada de adoptar una decisión (norma europea) y publicarla en el *Diario Oficial de la Unión Europea*, desde ese momento se establece la posibilidad —sin más requisitos— de realizar transferencias internacionales de protección de datos a dicho país.

Cuestión diferente son las normas corporativas vinculantes, que aplican en el ámbito de los grupos o las uniones de carácter empresarial. Estas ejercen una actividad económica conjunta e invocan este tipo de normas, previa autorización de parte de una de las autoridades de control de los Estados miembros de la Unión Europea, para poder realizar transferencias internacionales dentro de su grupo empresarial, respetando los principios y derechos establecidos por la normativa europea en materia de protección de datos de carácter personal.

III.3. Evaluaciones de impacto

Tal y como establece el considerando 90 del Reglamento General de Protección de Datos, las evaluaciones de impacto suponen un mecanismo a través del cual es posible valorar «La particular gravedad y probabilidad de alto riesgo de un tratamiento de datos determinado y siempre teniendo presente que dicha herramienta debe tener en cuenta el ámbito, la naturaleza, contexto y fines del tratamiento, así como los orígenes del riesgo» (Parlamento y Consejo Europeo, 2016, p. 17). Además, el considerando continúa detallando que la evaluación de impacto debe incluir «las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el Reglamento» (p. 17).

Como comenta la propia Agencia Española de Protección de Datos (2014), una evaluación de impacto es un «análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos» (p. 8).

Lo primero que debe ser matizado es que una evaluación de impacto no es igual a una auditoría en materia de protección de datos de carácter personal, pues una auditoría en materia de protección de datos de carácter personal es una «auditoría de cumplimiento». Por tanto, la misión de los auditores no es otra que la de emitir una opinión profesional sobre si una entidad u organización cumple con la legislación vigente en materia de protección de datos de carácter personal; mientras que una evaluación de impacto es algo más que una mera revisión del cumplimiento normativo. En esa línea, su objetivo esencial se centra no solo en la verificación del cumplimiento, sino también en cómo se satisfacen las expectativas de las personas y de la sociedad ante cualquier tratamiento de sus datos de carácter personal.

Tal y como establece la Agencia Española de Protección de Datos (2014, pp. 9-10), hay una serie de elementos comunes que forman parte del *core* de una evaluación de impacto en la materia que nos ocupa. Por ello, una vez analizados los elementos comunes, toca comentar cuándo

se considera que un responsable del tratamiento debe realizar una evaluación de impacto. Así, en el Reglamento General de Protección de Datos se establece que una evaluación de impacto debe realizarse cuando el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas.

No obstante, el Reglamento General de Protección de Datos deja abierta la posibilidad de que las autoridades nacionales de protección de datos, junto con el Comité Europeo de Protección de Datos, puedan proporcionar listas de casos en los que se supone obligatoria una evaluación de impacto. Sin embargo, y antes de continuar, queremos dejar apuntado que, aunque la norma habla de evaluaciones de impacto obligatorias, esto no implica que —conforme al principio de responsabilidad proactiva— un responsable del tratamiento no pueda realizar una evaluación de impacto de manera facultativa. Y esa es, quizá, la cuestión más importante para que los responsables del tratamiento procedan a aplicar determinadas herramientas de forma proactiva.

Dicho esto, la Agencia Española de Protección de Datos (2020, pp. 2-3)[7] ha publicado en su página web una lista de los tipos de tratamiento de datos que requieren evaluación de impacto. Por otro lado, debe tenerse en cuenta que las evaluaciones de impacto son procesos rigurosos y detallados que se componen de una serie de fases, cuyo correcto desarrollo implica precisamente el éxito de la evaluación de impacto. Las fases en las que podemos dividir una evaluación de impacto son las siguientes:

- Creación del equipo de trabajo.
- Descripción del proyecto y de los flujos de datos personales.
- Identificación y evaluación de riesgos.
- Consulta con las partes afectadas.
- Gestión de los riesgos identificados.
- Análisis de cumplimiento normativo.
- Redacción, publicación e integración del informe final
- Implantación de las conclusiones.
- Revisión de los resultados y realimentación de la evaluación de impacto (Agencia Española de Protección de Datos, 2014, pp. 17-49).

7 Los tratamientos que la Agencia Española de Protección de Datos considera que requieren de una evaluación de impacto pueden consultarse a través del siguiente enlace: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

Como podemos observar, las evaluaciones de impacto forman parte de esta «nueva» generación de mecánicas o sistemas que nos ayudan a adoptar, en el seno de una organización, el principio de responsabilidad proactiva que comentamos en el presente artículo. Ponemos las comillas en la palabra «nueva» para hacer ver, tal y como lo expresan perfectamente las autoridades de control de Argentina y Uruguay, que la novedad reside en su «inclusión como obligación expresa en algunas legislaciones de Latinoamérica, así como en la legislación europea» (Autoridades de Control de la República Oriental del Uruguay y de la República Argentina, 2020, p. 6).

III.4. Protección de datos desde el diseño y por defecto

En relación con la protección de datos desde el diseño y por defecto, lo primero que debemos destacar es que nos encontramos en presencia de un principio que dispone de dos facetas o caras.

Por un lado, estamos hablando del clásico principio de seguridad establecido en la gran mayoría de las normas de protección de datos de carácter personal. Por tanto, se trata de un principio extendido en el mundo y que, además, suele cumplirse con independencia de que se tenga o no una marcada sensibilización en materia de protección de datos. Al fin y al cabo, la seguridad en tecnologías informáticas (IT) es una de las necesidades básicas de cualquier organización no solo por protección de datos, sino por muchas otras cuestiones: ataques maliciosos, secretos empresariales, secretos de Estado, patentes, marcas y un largo etcétera hacen que el presente principio esté altamente presente en cualquier organización, tanto pública como privada.

Esta faceta del presente principio implica que el responsable del tratamiento se encuentra obligado a implementar políticas, medidas y protocolos, tanto de carácter técnico como organizativo, tendentes a garantizar la seguridad de los datos de carácter personal, y aquí radica en cierto modo la «novedad» desde el diseño y por defecto. Pero, ¿qué significa esto? Aquí entra en juego la segunda faceta del presente principio. La protección desde el diseño y por defecto implica que tanto las organizaciones públicas como privadas, y principalmente determinadas organizaciones sectoriales, deben alentar a la industria tecnológica a que, cuando se diseña y desarrolla cualquier tipo de producto, servicio o aplicación desde el cual se puedan tratar datos de carácter personal, lo hagan siempre pensando en las figuras más importantes de cualquier norma de protección de datos: los responsables y los encargados del tratamiento, de tal forma que estos puedan cumplir adecuadamente con la normativa en materia de protección de datos de carácter personal.

Como podemos observar, estamos hablando de una «actualización» del clásico principio de seguridad. Lo novedoso reside, desde nuestro

punto de vista, en que de forma implícita se está asimilando a los productores de tecnología a la figura del encargado del tratamiento o, en todo caso, incluso a la de corresponsable del tratamiento. Es decir, si se desarrolla una tecnología con la cual se van a tratar datos personales, esta cuestión debe ser tenida en cuenta en el desarrollo del producto, del servicio o de la aplicación concreta. Por tanto, si esta no se desarrolla en base al presente principio, los productores de tecnología pueden llegar a ser sancionados por la autoridad de control.

Con el antiguo principio de seguridad la responsabilidad penal, civil o administrativa recaía en exclusiva sobre la figura del responsable y del encargado del tratamiento. Desde luego, con la presente actualización, responsables y encargados no dejan de ser responsables, pero en cierto modo la industria tecnológica pasa a serlo también. La industria debe responsabilizarse de crear productos, servicios y aplicaciones respetuosas de la protección de datos de carácter personal; si no lo son, no solo el mercado les hará pagar el coste, sino que, en este caso, también las autoridades de control.

V. CONCLUSIÓN

Vivimos en la era del conocimiento, caracterizada por los gigantescos avances producidos en los campos de la informática y de las comunicaciones. Ambos sectores se han convertido en una ventaja táctica para cualquier organización, tanto pública como privada, que les permite maximizar sus beneficios a través del tratamiento de la información en general y del tratamiento de datos de carácter personal en particular.

En este contexto, una normativa de protección de datos «actual» necesita defender y garantizar los derechos y libertades de las personas. Sin embargo, en el escenario mundial, y más específicamente en el ámbito latinoamericano, las normativas distan mucho de ser actuales y conforme a las nuevas tecnologías y riesgos a los que se ven expuestos los datos de carácter personal. Las normativas de protección de datos sufren de obsolescencia con una rapidez nunca vista en el campo del derecho, tal es así que incluso el Reglamento General de Protección de Datos Europeo puede considerarse desfasado a pesar de ver la luz en el año 2016. Eso también es predicable en el ámbito latinoamericano, donde tenemos casos como el de la Ley 13709/18 en Brasil, de agosto de 2020, relativa a la protección de datos de carácter personal, la cual probablemente tampoco podrá responder con eficacia a los retos que enfrentará dentro de unos meses; o el caso de la normativa uruguaya, cuyo decreto N° 64/2020, aprobado en febrero de 2020 para reglamentar la ley de protección de datos personales (Ley N° 18.331), acaso tampoco será capaz de hacer frente a los desafíos que depara la protección de

datos. Argentina aún tiene pendiente que se trate en el Congreso un proyecto de ley en materia de protección de datos de carácter personal que busca adaptarse a los «nuevos tiempos», mientras que —como ya hemos comentado anteriormente— muchos países en Latinoamérica ni siquiera tienen una normativa en materia de protección de datos de carácter personal.

Si hay un atisbo de luz normativa, este reside en la implementación de sistemas alternativos a la normativa. En un mundo global donde las reacciones jurídicas solo son locales, la única esperanza para la protección de datos de carácter personal reside en mecánicas alternativas, sustitutivas del derecho, en las que los actores en materia de protección de datos de carácter personal en general, y los responsables del tratamiento en particular, decidan someterse a mecanismos que van más allá de la normatividad y cuya implicación no debe verse como una carga adicional, sino como una oportunidad. Sería, pues, una oportunidad de disponer de una correcta cultura de protección de datos de carácter personal en el seno de las organizaciones; una oportunidad para que los clientes, usuarios y otros colectivos tengan una sensación de confianza en las marcas; una oportunidad, en definitiva, de mejorar la reputación de las entidades con base en un tratamiento de datos serio, responsable y, sobre todo, cumplidor de la normativa.

Dicha oportunidad pasa por empezar a aplicar el principio de responsabilidad proactiva dentro de un entorno heterorregulador. Somos de la opinión de que dicho principio es especialmente importante en el ámbito latinoamericano, que es muy fraccionado desde el punto de vista normativo. Téngase en cuenta que existen países sin una normativa específica como Bolivia, Ecuador, El Salvador, Guatemala, Honduras o Venezuela; pasando por países cuyas normas son bien del siglo pasado, bien de estadios iniciales del siglo actual, como Argentina, Chile o Paraguay; o por naciones con leyes incluso anteriores al Reglamento General de Protección de Datos Europeo (que puede entenderse como la normativa más «moderna») como Colombia, Costa Rica, República Dominicana, Nicaragua o Perú. Únicamente Panamá, Uruguay y Brasil disponen de normativas promulgadas de forma íntegra —es decir, sin sufrir modificaciones en su texto original— después del año 2016.

Como podemos observar, el presente escenario, tan fragmentado, difícilmente puede plantar batalla a los retos jurídicos y tecnológicos a los que se enfrenta la protección de datos de carácter personal en la actualidad. Sin embargo, la solución no pasa por promulgar nuevas normas de protección de datos, pues ello no serviría para nada y, desgraciadamente, los Estados se verían obligados a cambiar la legislación cada dos o tres años sin que dicha solución garantice obtener unos resultados satisfactorios. La respuesta pasa, como ya hemos dicho, por

implementar nuevas mecánicas y, sobre todo, porque los responsables del tratamiento cambien la concepción que tienen actualmente sobre la protección de datos de carácter personal y el cumplimiento normativo, y pasen a aplicar el principio de responsabilidad proactiva en el seno de sus organizaciones.

Como hemos comentado a lo largo del presente artículo, el principio de responsabilidad proactiva puede ser eficaz en tanto no solo va a reducir el incumplimiento de las normativas en materia de protección de datos de carácter personal, sino que también se posiciona como una herramienta de mejora de la imagen y reputación de cualquier organización en la medida en que genera confianza en los actores relacionados a la protección de datos de carácter personal.

Desde el punto de vista latinoamericano, consideramos que si los responsables del tratamiento estiman este principio como una oportunidad y no como una carga —teniendo claro que adoptarlo no supone abandonar la senda del cumplimiento legislativo, sino todo lo contrario: aplicar un principio garantista a mayores—, los beneficios que podrían obtener compensarían sin duda alguna las cargas que la asunción del presente principio supone. Además, y como ya hemos puesto de manifiesto, el principio de responsabilidad proactiva se puede completar con una serie de herramientas útiles, especialmente en el ámbito latinoamericano. Las evaluaciones de impacto, las normas corporativas vinculantes, la protección de datos desde el diseño y por defecto, y la designación de un delegado de protección de datos, se tornan en herramientas esenciales para la asunción del principio de responsabilidad proactiva.

De lo que hablamos, en definitiva, es de que el responsable latinoamericano del tratamiento proceda a actuar en dos capas: la capa del cumplimiento normativo, a la cual viene obligado a fin de cuentas; y la capa facultativa, en donde el responsable del tratamiento, de forma proactiva, adopta en el seno de su organización algunos de los sistemas de responsabilidad que hemos mencionado en el presente artículo. Es decir, hablamos de un entorno heterorregulador.

Recordemos algo que los responsables latinoamericanos del tratamiento no deben pasar por alto: vivimos es un entorno global, un entorno en el que un responsable del tratamiento ya no cumple sus finalidades en un área local o nacional. Hoy día todo se ha convertido en global o, lo que es lo mismo, en internacional. Ante los retos globales, no cabe escudarse en cumplir con las normas locales pues el cumplimiento debe ser también global. Cuanto antes entiendan esto los responsables del tratamiento, antes verán el beneficio de implantar el principio de responsabilidad proactiva en el seno de sus organizaciones.

Insistimos, solo para cerrar el presente artículo: es cierto que lo realmente interesante sería disponer de una normativa internacional en materia de protección de datos de carácter personal. Incluso, podemos llegar a tener un pensamiento utópico y pensar, como Kant, que lo ideal sería tener en el mundo una «federación de Estados libres». Pero nuestra propuesta tiene los pies en el suelo: si ello llega, no será hoy ni mañana. En el presente, el principio de responsabilidad proactiva se torna como el mejor mecanismo para garantizar los derechos y libertades en materia de protección de datos de carácter personal.

REFERENCIAS

Agencia Española de Protección de Datos. (2014). *Guía para una evaluación de impacto en la protección de datos personales*. Madrid: Agencia Española de Protección de Datos.

Agencia Española de Protección de Datos. (26 de marzo de 2020). *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4)*. Recuperado de https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

Autoridades de Control de la República Oriental del Uruguay y de la República Argentina. (28 de enero de 2020). *Guía de Evaluación de Impacto en la Protección de Datos*. Autoridades de Control de la República Oriental del Uruguay y de la República Argentina. Recuperado de https://www.argentina.gob.ar/sites/default/files/guia_final.pdf

Burnett, R. (2009). *Outsourcing IT - The Legal Aspects: Planning, Contracting, Managing and the Law*. Reino Unido: Gower Publishing.

Comisión de las Comunidades Europeas. (2008). *Decisión de la Comisión de 3 de junio de 2008, por la que se adoptan disposiciones de aplicación relativas al Responsable de la Protección de Datos de conformidad con el art. 24, apartado 8, del Reglamento (CE) N° 45/2001*. Luxemburgo: Servicio de Publicaciones de la Unión Europea.

Consejo de Europa. (28 de enero de 1981). *Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Estrasburgo.

Gonzalo Quiroga, M. (2003). *Orden público y arbitraje internacional en el marco de la globalización comercial: arbitrabilidad y derecho aplicable al fondo de la controversia internacional*. Madrid: Dykinson.

Grupo de Trabajo del Artículo 29. (2003). *Transferencias de datos personales a terceros países: aplicación del arts. 26 (2) de la Directiva sobre protección de datos de la Unión Europea a las normas corporativas vinculantes*. Bruselas: Servicio de Publicaciones de la Unión Europea.

Grupo de Trabajo del Artículo 29. (2010). *Dictamen 3/2010 sobre el principio de responsabilidad*. Bruselas: Servicio de Publicaciones de la Unión Europea.

Lara Bueno, M. I. (2008). *Manual básico de revisión y verificación contable*. Madrid: Dykinson.

Magide Herrero, M. (2000). *Límites constitucionales de las administraciones independientes*. Madrid: Instituto Nacional de la Administración Pública.

Masuda, Y. (1980). *La sociedad informatizada como sociedad post-industrial*. Tokio: Institute for the Information Society.

Morgan, R., & Boardman, R. (2008). *Data Protection Strategy: Implementing Data Protection Compliance*. Reino Unido: Sweet and Maxwell.

Nieto Tamargo, A., & Iglesias González, F. (2000). *La empresa informativa*. Barcelona: Ariel.

Parlamento y Consejo Europeo. (18 de diciembre de 2000). Carta de los Derechos Fundamentales de la Unión Europea. *Diario Oficial de la Unión Europea*. Luxemburgo: Oficina de Publicaciones de la Unión Europea.

Parlamento y Consejo Europeo. (4 de mayo de 2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de la Unión Europea*, L119/1.

Pereña Brand, J. (1996). *Dirección y gestión de proyectos*. Madrid: Díaz de Santos.

Quan-Hasse, A., & Wellman, B. (2005). How Computer-Mediated Hyperconnectivity and Local Virtuality Foster Social Networks of Information and Coordination in a Community of Practice. En *Communities and Technologies 2005* (pp. 215-238). Doredrecht: Springer. https://doi.org/10.1007/1-4020-3591-8_12.

Quan-Hasse, A., & Wellman, B. (2006). Hyperconnected Net Work: Computer-Mediated Community in a High-Tech Organization. En C. Heckscher (ed.), *The Firm as a Collaborative Community: Reconstructing Trust in the Knowledge Economy* (pp. 281-333). Nueva York: Oxford University Press.

Rotondo Tornaría, F. (2019). El principio de responsabilidad y el Reglamento Europeo de Protección de Datos. *Informática y Derecho: Revista Iberoamericana de Derecho Informático*, (6), 135-152.

Sainz Moreno, F. (2004). *Estudios para la reforma de la administración pública*. Madrid: Instituto Nacional de la Administración Pública.

Santamaría Ramos, F. J. (2011). *El encargado independiente. Figura clave para un nuevo derecho de protección de datos*. Las Rozas: Wolters Kluwer España.

Santos García, D. (2005). *Nociones generales de la Ley orgánica de protección de datos*. Madrid: Tecnos.

Terceiro, J., & Matías, G. (2001). *Digitalismo. El nuevo horizonte sociocultural*. Madrid: Taurus-Santillana.

Trigo Chacón, M. (2005). *Multinacionales, globalización y terrorismo*. Madrid: Visión Libros.

Whetten, D., & Cameron, K. (2005). *Desarrollo de habilidades directivas*. México: Pearson Educación.

Recibido: 27/03/2020
Aprobado: 20/07/2020